Référentiel de certification des systèmes d'encaissement

Réf. rédacteur : LNE/CITI/CH

Révision n° 1.4 – janvier 2019

Approbation LNE : 24/01/2019

Laboratoire national de métrologie et d'essais • Etablissement public à caractère industriel et commercial
Siège social : 1, rue Gaston Boissier - 75724 Paris Cedex 15 • Tél. : 01 40 43 37 00 - Fax : 01 40 43 37 37
info@lne.fr • lne.fr • RCS Paris 313 320 244 - NAF : 7120B - TVA : FR 92 313 320 244

Table des matières

Révisions du document

Version	Date	Motif de la mise à jour
1	29/11/2016	Version initiale
1.1	07/12/2016	Précisions apportées aux chapitres I.3/ domaine d'application (exclusion de la monétique) et V.4 / comité de marque (suppression du président et ajout de l'impossibilité de droit de veto conformément à la norme NF X50-067) suite au 1er comité de marque du 06/12/2016.
1.2	12/12/2016	Ajustement de la composition du comité de marque (V.4). Ajustement de la procédure de recours et de plainte (VI).
1.3	PROJET	Ensemble du document : Prise en compte de la FAQ de la DGFIP sur les logiciels de caisse sécurisés datée du 28/07/2017 § I.3 : précisions apportées au domaine d'application du référentiel §II.2 : prise en compte du retour d'expérience pour la rédaction des conditions § III : précisions apportées sur la marque LNE Système de caisse et sur les engagements des titulaires de certifications § IV : précisions apportées sur les modalités d'évaluation initiale et de surveillance. Glossaire : ajout de définitions
1.4	24/01/219	• Prise en compte des changements de la version mise à jour du 04/07/2018 du BOI-TVA-DECLA-30-10-30 o Inclusion des précisions issues de la FAQ du 28 juillet 2017 o Utilisation d'un format d'archives ouvert o Obligation de proposer 3 niveaux de clôture o Redéfinition du système d'encaissement o Précisions sur les données concernées o Obligation de tracer les opérations du purge/archivage • Réorganisation des différentes parties du référentiel • Clarification sur la différence certification/attestation • Précisions sur le processus de certification • Refonte des exigences qualité • Réorganisation des exigences techniques • Ajout de l'identifiant de l'établissement dans les données concernées • Ajout de la sécurisation des justificatifs • Mise à jour des exemples de solutions acceptables dans les mécanismes garantissant l'inaltérabilité des données

Chapitre I : Généralités

I.1) Objet & assujettis à la TVA concernés

Afin de lutter contre la fraude à la TVA liée à l'utilisation de systèmes permettant la dissimulation de recettes, la loi de finances pour 2016 a instauré l'obligation pour tous les professionnels assujettis à la TVA, qui effectuent des livraisons de biens et des prestations de service à destination de clients particuliers, enregistrant les paiements reçus en contrepartie au moyen d'un système de caisse, que celui-ci soit sécurisé. Ce système doit ainsi être certifié par un organisme indépendant accrédité par le COFRAC ou attesté par l'éditeur comme étant conforme à la règlementation fiscale, par le biais de l'attestation individuelle[1].

Cette obligation touche tous les secteurs d'activités, étant rappelé que la loi de finances pour 2018 a exclu du dispositif les assujettis à la TVA bénéficiant du régime de la franchise en base, ceux soumis au régime du remboursement forfaitaire de TVA agricole, ceux effectuant exclusivement des opérations exonérées de TVA[2] et ceux qui réalisent l'intégralité de leurs opérations entre professionnels uniquement (B to B).

Le présent référentiel décrit les modalités de certification des systèmes d'encaissement. Il s'appuie principalement sur l'article 88 de la loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016 et le bulletin officiel des finances publiques BOI-TVA-DECLA-30-10-30-20180704, qui définit les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données de transaction auxquelles le système doit se satisfaire. Le référentiel vise à certifier ces 4 caractéristiques, la caractérisation du périmètre fiscal du système et des versions du système, la documentation afférente au système, et l'organisation (SMC[3]) mise en place pour assurer la production et la livraison de systèmes d'encaissement conformes à la version certifiée.

I.2) Domaine d'application : définition du système d'encaissement

Un système d'encaissement est un système informatique (quelle que soit sa qualification : gestion, CRM, comptabilité, de caisse etc..) doté d'une fonctionnalité de caisse.

Une fonctionnalité de caisse consiste à mémoriser **et** à enregistrer extra-comptablement des paiements reçus en contrepartie d'une vente de biens ou de prestations de services, et ce quel que soit le moyen de paiement. On entend par enregistrer extra-comptablement que le paiement enregistré par le système **ne génère pas** simultanément, automatiquement, obligatoirement et sans intervention humaine une écriture comptable dans le système de comptabilité[4].

Certaines exclusions spécifiques existent. Il convient de se référer au BOI-TVA-DECLA-30-10-30. Le LNE n'a pas vocation à trancher sur l'applicabilité de ce BOI quant au système concerné.

[1] BOI-TVA-DECLA-30-10-30-20180704 : point 1.
[2] BOI-TVA-DECLA-30-10-30-20180704 : point 25.
[3] SMC : Système de Management de la Conformité
[4] BOI-TVA-DECLA-30-10-30-20180704 : point 30.

I.3) Attestation ou certification ?

La certification est une procédure par laquelle une tierce partie, l'organisme certificateur, donne une assurance écrite qu'un système d'organisation, un processus, une personne, un produit ou un service est conforme à des exigences spécifiées dans une norme ou un référentiel. Elle est encadrée par le Code de la Consommation.
Elle ne doit pas être confondue avec l'attestation individuelle fournie par l'éditeur lui-même, qui est une déclaration par laquelle l'éditeur témoigne et s'engage à ce que le système d'encaissement qu'il fournit respecte les conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données de transaction.

Dans le cadre de la loi des finances pour 2016, la certification de produit par un organisme accrédité est obligatoire pour les assujettis à la TVA éditant leur propre système d'encaissement[5].

[5] BOI-TVA-DECLA-30-10-30-20180704 : point 375.

Chapitre II : Processus d'attribution de certificat

II.1) Processus de commande

Après une première prise d'informations et d'échanges, le service commercial du LNE fait parvenir le questionnaire initial au demandeur de la certification qui doit être retourné rempli afin de pouvoir établir le devis. Le service commercial fait alors parvenir l'offre de certification au demandeur. Une fois la commande enregistrée, le processus de certification peut démarrer.

II.2) Processus de certification

Le processus de certification se découpe en plusieurs étapes successives. Les principales sont :

1. l'instruction du dossier de demande : l'examen de recevabilité documentaire ;
2. la réalisation de l'audit de certification :
   Il se découpe en 4 évaluations d'une durée minimale d'un jour chacune :
   - l'audit organisationnel destiné à s'assurer de la conformité du SMC mis en place aux exigences du chapitre III ;
   - l'évaluation de la conformité documentaire du système aux exigences du chapitre IV ;
   - l'évaluation de la conformité fonctionnelle du système aux exigences du chapitre IV ;
   - l'évaluation de la conformité robustesse du système aux exigences du chapitre IV ;
3. le retour sur les fiches de non-conformité le cas échéant ;
4. la prise de décision de certification en comité de lecture ;
5. l'émission du certificat une fois la décision de certification entérinée.

II.2.1) Examen de recevabilité documentaire

Une fois la prise de commande enregistrée, le LNE envoie au demandeur de la certification le formulaire de recevabilité documentaire.

Ce formulaire doit être retourné au LNE rempli et accompagné du dossier technique constitué de la documentation relative au système. Cette documentation doit être complète et décrire précisément l'ensemble des fonctionnalités et mécanismes mis en œuvre dans le cadre de la mise en conformité, permettant de répondre aux exigences techniques du référentiel LNE[6].

L'examen de recevabilité documentaire n'est pas équivalent à l'évaluation documentaire effectuée lors de l'audit de certification.

L'examen de recevabilité documentaire consiste à déterminer si l'évaluation de la conformité du système d'encaissement est possible compte tenu du degré d'aboutissement du dossier technique transmis par le demandeur. Pour ce faire il est constaté :

- si des documents demandés à l'exigence n° 1 du chapitre IV sont manquants ;
- si tout ou partie de la documentation règlementaire n'est pas en français ;
- si le périmètre fiscal et la gestion des numéros de version sont bien définis ;

[6] CF : Chapitre IV : exigences techniques applicables au système d'encaissement certifié

- si le principe des méthodes proposées pour répondre aux exigences du chapitre IV est pertinent.

A l'issue de l'examen de recevabilité documentaire, le LNE informe le demandeur du résultat.

Dans le cas où cette étape conclue à l'irrecevabilité du dossier, il appartient au demandeur de la certification de répondre au LNE en fournissant les documents manquants. Un devis complémentaire sera adressé par le service commercial du LNE si un second examen de recevabilité documentaire est nécessaire.

II.2.2) Planification de l'audit de certification

Dans le cas où l'examen de recevabilité documentaire est satisfaisant, le dossier est recevable et le LNE prend contact avec le demandeur, afin de définir les lieux et dates des différentes étapes de l'audit.

La durée de l'audit organisationnel peut être augmentée s'il est nécessaire de se déplacer sur plusieurs sites, si des sous-traitants interviennent dans la conception, le développement, les tests, la configuration/installation du système à certifier et ne sont pas suivis par le titulaire de la certification, ou encore s'il est nécessaire de faire appel à un interprète. Elle est fixée par défaut à une journée. Elle peut être diminuée sous réserve de justifier que le demandeur de la certification dispose d'un SMQ certifié ISO 9001 pour les activités couvertes par le référentiel.

La durée des évaluations documentaire, fonctionnelle et de robustesse d'un système d'encaissement est liée à sa complexité ; elle est fixée par défaut à une journée par évaluation. Elle peut être augmentée, notamment à l'issue de l'examen de recevabilité documentaire, selon la complexité du système d'encaissement (plusieurs interfaces homme/machine, configurations et/ou flux de données à tester, architecture du système etc.).

II.2.3) Réalisation de l'audit de certification

Plusieurs évaluations peuvent avoir lieu en même temps en fonction de la composition de l'équipe d'audit.

Il est rappelé que l'activité d'audit est basée sur un échantillonnage des informations disponibles. L'absence de non-conformité constitue une présomption et non une preuve de conformité aux exigences auditées.

II.2.3.1): Audit organisationnel

Le demandeur de la certification doit mettre en œuvre un Système de Management de la Conformité (SMC) destiné à s'assurer que chaque système d'encaissement, ou mise à jour, déployé répond aux exigences du chapitre IV.

Les exigences applicables à ce SMC sont définies au chapitre III et leur bonne application est vérifiée lors de l'audit organisationnel.

L'audit organisationnel du SMC a lieu chez le demandeur, de préférence sur le site où ont lieu les activités de conception, développement et tests concernant le système à

certifier. Lorsqu'un titulaire souhaite certifier plusieurs systèmes d'encaissement, l'audit organisationnel est mutualisé pour l'ensemble des systèmes.

Le demandeur de la certification doit s'assurer de la disponibilité d'un interlocuteur maitrisant le SMC mis en place, l'organisation de la société et ses processus, ainsi que de toute autre personne jugée pertinente.

II.2.3.2) Evaluation de la robustesse

L'évaluation de la robustesse du système d'encaissement a pour objectif de vérifier le respect des exigences de robustesse définies au chapitre IV. Le demandeur de la certification doit s'assurer de la disponibilité d'un :

- expert technique maîtrisant la conception, le développement/fabrication (connaissant le code source), la configuration et l'utilisation du système d'encaissement à certifier ;
- système d'encaissement fonctionnel dans un environnement de test (pour pouvoir notamment modifier la date du système facilement) avec tous les périphériques associés (Imprimantes, afficheurs, télécommande..), raccordés et fonctionnels, et des éventuelles connexions ou configurations possibles (à un PC, serveur ou tout autre système centralisé) ;
- système d'encaissement dans un environnement de développement (avec accès intégral au code source, accès direct aux bases de données, serveurs etc.) ;
- accès aux documentations utilisateur et technique.

II.2.3.3) Evaluation documentaire

L'évaluation documentaire du système d'encaissement a pour objectif de vérifier le respect des exigences documentaires définies au chapitre IV. Le demandeur de la certification doit s'assurer de la disponibilité de :

- un interlocuteur maîtrisant la documentation et la conception du système d'encaissement à certifier ;
- la documentation règlementaire[7] en français ;
- la documentation complémentaire[8] en français ou en anglais ;
- l'ensemble de la documentation à destination de l'évaluateur, ainsi que d'un moyen de transfert pertinent. Ces documents seront conservés par le LNE comme preuves d'audit.

II.2.3.4) Evaluation fonctionnelle

L'évaluation fonctionnelle du système d'encaissement a pour objectif de vérifier le respect des exigences fonctionnelles définies au chapitre IV. Le demandeur de la certification doit s'assurer de la disponibilité d'un :

- interlocuteur maîtrisant la conception, le développement/fabrication, la configuration et l'utilisation du système d'encaissement à certifier ;
- système d'encaissement fonctionnel dans un environnement de test (pour pouvoir notamment modifier la date du système facilement) avec tous les périphériques associés (Imprimantes, afficheurs, télécommande..), raccordés et fonctionnels, et des éventuelles connexions ou configurations possibles (à un PC, serveur ou tout autre système centralisé) ;

[7] CF : Chapitre IV exigence 1
[8] CF : Chapitre IV exigence 2

- jeu de données d'encaissement suffisamment fourni pour pouvoir réaliser les cas de test du référentiel : clôtures périodiques (journalière, mensuelle et annuelle), synchronisation des données, archivage, etc.

II.2.4) Réponse aux fiches de non-conformité

Dans le cas où une non-conformité est constatée durant une des étapes de l'audit de certification, une fiche décrivant la NC[9] est rédigée par l'évaluateur[10]/auditeur[11]. Celle-ci est transmise par le RE[12] au demandeur de la certification, lors de la réunion de clôture de l'audit de certification.

On distingue 2 catégories de NC :

1) NC 'système' du SMC (chapitre III)

   Elles peuvent être mineures ou majeures.

   Une NC majeure est bloquante pour la certification : elle devra être corrigée avant la certification.

   Une NC mineure n'est pas bloquante pour la certification mais devra être corrigée avant le prochain audit de suivi, sous peine de suspension de certificat.

2) NC 'produit' du système d'encaissement (chapitre IV)

   Toute NC produit est bloquante pour la certification : elle devra être corrigée avant la certification.

   Si la NC est uniquement documentaire, le RE ou le LNE peuvent la lever après transmission des documents appropriés.

Le demandeur de certification a alors un délai fixé par le RE (de minimum 3 semaines) pour lui retourner chaque fiche complétée par l'analyse de la NC et l'action engagée.

Après analyse des actions proposées par le demandeur de la certification, le RE se prononce sur sa pertinence et préconise le type de suivi nécessaire à la NC.

II.2.5) Avis du Responsable d'évaluation et revue du rapport

Après réception des éventuelles fiches de NC complétées par le demandeur de la certification et le RE, le LNE analyse le rapport d'évaluation et l'avis du responsable d'évaluation. A la lecture du rapport il peut demander des informations complémentaires au demandeur de la certification, avant le passage en comité de lecture.

II.2.6) Décision du comité de lecture

Le comité de lecture est chargé de rendre un avis sur la décision de certification dans le processus d'attribution, de surveillance, de retrait ou de suspension des certificats. Il est composé au minimum :

- d'un représentant de la direction du LNE (qui ne peut intervenir en tant que chef de projet certification et n'ayant pas participé à l'évaluation) ;
- d'un chef de projet certification n'étant pas en charge du dossier ;
- d'un chef de projet certification en charge de présenter le dossier.

[9] NC : Non-conformité

[10] Evaluateur pour les étapes 2/3/4 : évaluations du système d'encaissement (chapitre IV)

[11] Auditeur pour l'étape 1 : audit organisationnel sur le système de management de la conformité (chapitre III)

[12] RE : responsable d'évaluation

Le comité est présidé par le représentant de la direction du LNE et a pour mission :

- d'examiner les rapports d'évaluation et de formuler un avis et une recommandation sur les décisions à prendre, notamment sur le type et la durée du suivi d'une NC ;
- le cas échéant, d'examiner dans un premier temps les appels contre les décisions du LNE et de formuler un avis sur les suites à donner ;
- d'évaluer la qualité des rapports d'évaluation.

La décision de certification s'appuie sur l'examen des éléments du dossier et du rapport de l'audit de certification. Chaque décision de certification est matérialisée par l'enregistrement et le cas échéant l'émission d'un certificat.

Les certificats sont émis sans date limite de validité et restent valides tant qu'aucune modification portant sur les caractéristiques certifiées (périmètre fiscal) n'est apportée. Il appartient à l'entreprise de signaler au LNE les modifications afin de faire réaliser les évaluations nécessaires à la révision du certificat.

II.3) Surveillance du certificat

Il est procédé à une évaluation de surveillance annuelle. Le contenu de l'évaluation annuelle varie selon les cas ; sa durée ne peut être inférieure à une journée.

Afin de planifier cette surveillance, le LNE envoie un questionnaire à l'entreprise dont le système est certifié afin de connaitre les évolutions depuis l'évaluation précédente. Une fois le questionnaire retourné, le LNE établit une offre de surveillance en fonction des modifications effectuées.

Les modalités d'évaluation en fonction des modifications lors du suivi sont les suivantes :

- **Si le système certifié n'a subi aucune modification :**
  L'audit de suivi annuel porte sur l'audit du SMC du titulaire et des vérifications destinées à s'assurer de l'absence de modification du système (comparaison de l'empreinte). Il dure 1 journée. Le but de l'évaluation est de s'assurer que le SMC est maintenu, afin de produire des systèmes d'encaissement identiques à celui certifié et que la traçabilité des systèmes distribués est assurée.

- **Si le système certifié a subi une modification de son périmètre fiscal** (et donc un changement de version majeure) :
  L'audit de suivi annuel est considéré par défaut comme une évaluation initiale avec examen de l'ensemble des exigences documentaires, fonctionnelles et de robustesse, listées au chapitre IV ainsi que les exigences organisationnelles liées au SMC, listées au chapitre III. Sa durée est fonction des modifications apportées au système.

  Note : en cas de modification sur le périmètre fiscal, l'entreprise doit informer le LNE des modifications effectuées avant de pouvoir distribuer cette version. En effet le certificat ne couvre le système que pour une version majeure donnée.

- **Si le système certifié a subi une modification mineure** (donc sans changement sur le périmètre fiscal) :

L'audit de suivi annuel porte sur l'audit du SMC du titulaire et des vérifications fonctionnelles permettant de s'assurer que les versions mineures ultérieures du système d'encaissement continuent de répondre aux 4 conditions sur les données d'encaissement définies par le BOI[13], et sur l'absence de modification du périmètre fiscal du système (comparaison de l'empreinte). Il dure 2 jours.

Une fois la commande passée, les étapes ci-dessous sont identiques à celles de l'audit de certification initial :

1. planification de l'audit de suivi ;
2. réalisation de l'audit de suivi (selon les modalités d'évaluation précédentes) ;
3. réponses aux éventuelles fiches de NC ;
4. revue du rapport ;
5. décision du comité de lecture.

[13] BOI-TVA-DECLA-30-10-30-20180704 : point 330.

Chapitre III : Exigences applicables au système de management de la conformité (SMC)

Le demandeur/titulaire de la certification doit mettre en œuvre, évaluer et maintenir à jour un Système de Management de la Conformité (SMC) destiné à s'assurer que chaque système d'encaissement ou mise à jour mis sur le marché répond en permanence aux exigences du présent référentiel.

Ce SMC doit respecter les exigences définies ci-dessous.

Note : toute mention future à l'action d'enregistrer une information ou de produire un enregistrement fait référence aux exigences du III.14) du présent chapitre.

III.1) Contexte

L'organisme doit déterminer et enregistrer les enjeux internes et externes ainsi que les risques (juridiques, réputation, financiers, etc.) liés à la conformité des systèmes d'encaissement mis sur le marché.

Pour ce faire, l'organisme doit notamment prendre en compte les contextes externes règlementaires, économiques mais aussi le contexte interne de l'organisme (ressources, processus, fournisseurs, sous-traitants etc.). Cela peut par exemple être fait en mettant en œuvre un processus de management des risques, en établissant une cartographie des risques ou une analyse SWOT.

III.2) Engagements et responsabilités de l'entreprise

Les entreprises certifiées sont seules responsables de la conformité de leurs produits, les contrôles du LNE ne pouvant se substituer à leurs responsabilités.

Les entreprises, pour les produits certifiés, s'engagent à :

- réaliser exclusivement des systèmes d'encaissement conformes au présent référentiel de certification ;
- s'assurer que tous les systèmes d'encaissement certifiés distribués continuent de répondre aux exigences qui les concernent ;
- mettre en œuvre les changements appropriés en cas de nouvelles exigences ;
- prendre toutes les dispositions nécessaires pour la réalisation des évaluations initiales et de surveillance :
    - transmission du dossier technique et le cas échéant des échantillons nécessaires, accès aux sites, zones, personnels et sous-traitants le cas échéant concernés par l'évaluation,
    - instruction des non conformités formulées dans les rapports d'évaluation,
    - participation d'observateurs le cas échéant,
- ne communiquer que des informations loyales et sincères ;
- informer sans délai le LNE des changements pouvant avoir des conséquences sur la conformité du système ou la validité de la certification émise (changement de statut juridique, modification/mise à jour du système certifié, etc.).

III.3) Rôles et responsabilités

La direction doit confier et communiquer la responsabilité et l'autorité à la fonction en charge de la conformité pour:

a) s'assurer que le système de management de la conformité est conforme au présent chapitre III ;
b) analyser les exigences techniques définies au chapitre IV ;
c) les décliner en spécifications fonctionnelles, pouvant être mise en œuvre ;
d) assurer ou organiser des sessions de formation/information pour les employés concernés afin de s'assurer qu'ils soient conscients des exigences de conformité qui les concernent ;
e) définir des indicateurs de performance de la conformité ;
f) contrôler et mesurer ces indicateurs ;
g) analyser les résultats pour identifier si des actions correctives sont nécessaires ;
h) identifier et gérer les risques liés à la conformité relatifs aux tierces parties telles que fournisseurs, agents, distributeurs, consultants et sous-traitants ;
i) superviser les conditions d'externalisation, afin de s'assurer qu'elles tiennent compte des exigences de conformité définies dans le présent référentiel.

La direction doit s'assurer que les responsabilités et autorités, pour chaque activité en lien avec les systèmes d'encaissement, soient définies de façon à assurer que les exigences définies dans le présent référentiel sont, systématiquement, et de façon permanente, mises en œuvre.

III.4) Objectifs et mise en œuvre du SMC

L'organisme doit prendre en compte les enjeux, risques et exigences du présent référentiel pour définir les objectifs du SMC et les décliner à chaque niveau et fonction en objectifs de conformité pour les activités de conception, développement, contrôles, distribution, configuration, installation et évaluation et traitement des NC.

Ces objectifs de conformité doivent être :

- pertinents ;
- cohérents avec les objectifs du SMC ;
- mesurables ;
- communiqués aux personnes concernées ;
- compris et appliqués ;
- surveillés régulièrement par une personne en charge de la conformité ;
- mis à jour si nécessaire ;
- enregistrés.

L'organisme doit s'assurer que le SMC peut atteindre les résultats attendus et prévenir ou réduire les risques. Pour cela, il doit notamment prévoir :

- les actions pertinentes à mettre en œuvre en corrélation avec
  - les enjeux ;
  - les risques ;
  - les exigences ;
- l'intégration de ces actions au sein des activités concernées ;
- l'évaluation (et son enregistrement) de l'efficacité de ces actions.

III.5) Mise à jour du SMC

Le contexte évoluant, l'organisme doit être en mesure d'identifier les nouveautés et changements de législation, directives, règlementations, exigences de conformité afin d'assurer la pérennité de la conformité des systèmes d'encaissement.

L'organisme pourra par exemple :

- être destinataire des bulletins d'information des organismes de règlementation (DGFIP, ministères, etc.) et de certification (LNE) ;
- suivre ou participer à des groupes de travail professionnels ;
- s'abonner aux newsletters appropriées ;
- participer aux évènements professionnels du secteur ;
- consulter régulièrement les sites internet des organismes de règlementation et de certification ;
- faire appel à des conseillers juridiques ;
- etc.

L'impact de ces changements doit être évalué et les actions (et modifications du SMC) qui en découlent doivent être effectuées, suivies et enregistrées. En cas de modification des exigences, les spécifications fonctionnelles devront clairement les identifier.

III.6) Etablissement des contrôles de conformité

L'organisme doit :

- mettre en œuvre et enregistrer des contrôles efficaces pour chaque activité liée au système d'encaissement (conception, développement, intégration, configuration/installation) afin de s'assurer que les exigences sont respectées et que les non-conformités sont évitées ou détectées et corrigées ;
- désigner des personnes compétentes, maitrisant les exigences du référentiel pour effectuer ces contrôles ;
- enregistrer les résultats de ces contrôles ;
- en cas de non-conformité, enregistrer l'analyse de la cause et les actions prises afin de corriger la NC ;
- s'assurer que les contrôles définis ont bien été réalisés aux étapes opportunes et que les résultats démontrent la conformité du système d'encaissement au présent référentiel.

Ces contrôles peuvent s'appuyer sur :

- des politiques, procédures, processus et instructions de travail opérationnels documentés, clairs, pratiques et faciles à suivre ;
- des systèmes et des rapports d'anomalies ;
- des approbations ou revues de code ;
- des plans et rapports de test ;
- une séparation des rôles et des responsabilités incompatibles ;
- des processus automatisés ;
- des plans annuels de conformité ;
- des audits de la conformité.

III.7) Conception et développement du système d'encaissement

L'organisme doit mettre en œuvre, de façon maitrisée, et enregistrer un processus de conception et un processus de développement du système d'encaissement ou de sa mise à jour approprié pour assurer la fourniture de systèmes d'encaissement conformes aux exigences du présent référentiel.

Les éléments de sortie du processus de conception qui doivent être enregistrés sont, a minima, l'ensemble des spécifications fonctionnelles liées à la conformité au présent référentiel et les plans de tests associés.

L'élément de sortie du processus de développement est un prototype ou une mise à jour d'un système d'encaissement, conforme au présent référentiel ainsi qu'à minima l'enregistrement des rapports des tests de conformité.

Les éléments suivants du processus de développement doivent être définis et enregistrés :

- la méthode de développement suivie (cycle en V, W, méthode agile, méthode propre à l'organisme, etc.) ;
- la gestion du code source : explication de l'organisation des répertoires, fichiers de code source, classes, packages, librairies, dll, etc. ;
- le périmètre fiscal du système d'encaissement[14] ;
- la gestion de la nomenclature des versions (et notamment la gestion des numéros de versions majeures et mineures)[15].

Ces processus doivent prendre en compte :

- les exigences de conformité du présent référentiel ;
- la revue des spécifications fonctionnelles et des rapports de tests par la fonction en charge de la conformité.

La maîtrise de ces processus doit notamment s'appuyer sur l'atteinte et l'enregistrement des objectifs et contrôles de conformité définis au préalable et sur la mise en œuvre, le suivi et l'enregistrement de toute action jugée nécessaire pour remédier aux problèmes identifiés lors des contrôles.

En cas de modification des processus de conception et/ou de développement, l'organisme doit s'assurer, et enregistrer les preuves, que la modification n'a pas d'impact négatif sur la conformité du système d'encaissement au présent référentiel.

III.8) Maitrise des sous-traitants

La sous-traitance de certaines activités (conception, développement, fabrication, tests, configuration, installation) liées au système d'encaissement est possible à condition qu'elle, ainsi que les risques sur la conformité du système d'encaissement, soient maitrisés.

Pour cela, les conditions de sous-traitance doivent être formalisées et enregistrées (définition du sous-traitant, exigences, objectifs et contrôles de conformité, communication des résultats, procédure à suivre en cas de non-conformité).

[14] CF : exigence technique n° 20
[15] CF : exigence technique n° 21

Le sous-traitant doit s'engager à respecter les exigences du présent référentiel.

L'organisme doit surveiller les conditions de sous-traitance ainsi que les résultats (et les enregistrer) de l'activité externalisée en mettent en œuvre des contrôles afin de s'assurer du maintien de la conformité du système d'encaissement. Il doit communiquer ces modalités de contrôle/évaluation au sous-traitant concerné.

Il est par exemple possible de suivre ces conditions via un audit du système de management de la qualité du sous-traitant par le LNE ou de tenir compte d'une certification ISO 9001 par un organisme accrédité sur les activités sus-citées liées aux systèmes d'encaissement et les sites concernés.

L'organisme doit identifier ses fournisseurs/sous-traitants critiques, analyser les risques sur la conformité du système d'encaissement liés à la sous-traitance et mettre en œuvre toutes les actions jugées nécessaires afin de réduire ces risques. Ces informations doivent être enregistrées.

III.9) Identification et traçabilité de la distribution

Chaque système d'encaissement distribué doit être identifié de manière unique (ainsi que la version distribuée). Cette identification doit permettre :

- d'assurer la traçabilité des systèmes distribués sur le marché ;
- de pouvoir faire une mise à jour ou une nouvelle installation le cas échéant (vulnérabilité majeure détectée, changement d'exigences de conformité à appliquer, etc.).

L'organisme doit enregistrer et mettre continuellement à jour un registre des systèmes et versions distribués à ses clients.

III.10) Communication avec les clients

L'organisme doit transmettre au client chez qui le système d'encaissement certifié est installé :

- tous les documents nécessaires au bon fonctionnement du système d'encaissement (mode d'emploi, prérequis matériel, etc.), que ceux-ci soient fournis par l'éditeur/fabricant ou un distributeur ;
- les procédures de support et de formation le cas échéant ;
- les engagements de responsabilité des clients vis-à-vis de la loi des finances pour 2016 (obligation de réaliser les clôtures, conservation des données, etc.) ;
- une description du moyen d'accès aux données d'encaissement par l'administration fiscale ainsi que d'un manuel utilisateur à destination de l'administration fiscale décrivant le moyen d'accès aux données d'encaissement, une description du format présenté, et la manière de procéder à la vérification d'intégrité des données[16] ;
- le certificat correspondant.

[16] CF : exigence technique n° 19

Par ailleurs, il doit s'assurer de la disponibilité des documents précités pour les équipes internes et les utilisateurs pendant 3 ans après la date de fin de distribution du système d'encaissement certifié.

La communication concernant la certification du système d'encaissement ne doit pas :

- être ambiguë pour le client quant au nom et à la version du système d'encaissement bénéficiaire de la certification ;
- porter à confusion sur le fait que la certification concerne un système d'encaissement et non une entreprise, un système de management ou une prestation de service.

La liste des systèmes de caisse certifiés est disponible sur le site internet du LNE via une recherche dans le moteur dédié (https://www.lne.fr/recherche-certificats) : sélectionner comme système « LNE Produits ». Le LNE fournit sur demande les informations relatives à la validité d'un certificat donné.

III.11) Usage de la marque LNE – Système de caisse

L'entreprise qui a un ou plusieurs de ses systèmes de caisse certifiés peut utiliser le logo « LNE système de caisse » sur ses supports de communication.

Lorsque le demandeur/titulaire prévoit l'apposition du marquage LNE (logo LNE – système de caisse), il doit respecter les dispositions destinées à s'assurer du bon usage de la marque :

- ne pas utiliser la certification obtenue d'une manière qui puisse nuire au LNE, ni faire de déclaration ou de communication sur la certification de ses produits qui puisse être considérée comme trompeuse ou non autorisée ;
- toute référence à la certification avant la notification de celle-ci est interdite ;
- en cas de retrait de certification ou d'échéance de validité, la référence à cette certification retirée ou échue est interdite : tout moyen de communication qui y fait référence doit cesser d'être utilisé ;
- faire des déclarations sur la certification en cohérence avec le certificat émis par le LNE ;
- reproduire les certificats dans leur intégralité, avec les annexes le cas échéant, en cas de fourniture à un tiers ;
- toute référence à la certification LNE systèmes de caisse dans la publicité, la présentation de tout service, ainsi que sur les documents commerciaux de toute nature qui s'y rapportent doit reprendre au minimum les informations suivantes :
    - le numéro du certificat ;
    - l'adresse du site internet du LNE.

Tout usage ou référence abusif de la marque/certification LNE systèmes de caisse, qu'il soit l'objet du titulaire du certificat ou d'un tiers, fera l'objet de poursuites en application de la réglementation en vigueur concernant la publicité mensongère et la propriété intellectuelle.

III.12) Evaluation et amélioration des performances du SMC

L'organisme doit mettre en œuvre une surveillance du SMC, qui consiste en la collecte et l'analyse d'informations dans le but d'évaluer et améliorer l'efficacité du SMC.

Cette surveillance comprend l'évaluation de l'efficacité :

- des contrôles définis en III.6, par exemple par analyse des résultats de tests par échantillonnage ;
- du traitement des non-conformités précédemment identifiées ;
- des actions mises en œuvre pour réduire les risques liés à la conformité des systèmes d'encaissement distribués ;
- des prestataires externes.

L'organisme doit tirer parti de la surveillance de système de SMC afin de déterminer, mettre en œuvre et enregistrer toute action jugée pertinente permettant l'amélioration du SMC et la réduction des risques de NC.

III.13) Traitement des non-conformités

Il ne peut exister aucune dérogation aux exigences du présent référentiel.

L'organisme doit s'assurer que les systèmes d'encaissement non-conformes produits soient identifiés et maitrisés afin d'éviter leur distribution et utilisation.

L'organisme doit réagir (même après distribution éventuelle) à une non-conformité de la manière suivante :

- analyser la NC : identifier ses causes afin de déterminer s'il est nécessaire de mener une action pour les éliminer afin que la NC ne se reproduise pas ;
- mettre en œuvre les actions permettant :
    - de corriger la NC ;
    - ou d'empêcher l'utilisation du ou des systèmes d'encaissement concernés, de prévenir ses clients, et procéder au rappel des produits ou à leur mise à jour ;
- évaluer l'efficacité des actions mises en œuvre ;
- mettre à jour les risques identifiés en III.1 si nécessaire ;
- mettre à jour le SMC tel que décrit en III.5 si nécessaire.

L'organisme doit enregistrer les informations concernant la nature de la NC, son analyse, les actions mises en œuvre ainsi que leurs résultats.

III.14) Gestion des enregistrements

L'organisme doit maîtriser les enregistrements cités dans le présent référentiel ainsi que tous ceux jugés pertinents afin qu'ils soient disponibles, accessibles et conviennent à l'utilisation, quand et là où ils sont nécessaires. L'organisme doit s'assurer, du stockage, de la protection, de la durée de conservation et de l'élimination de ces enregistrements.

Les enregistrements concernés sont a minima les suivants :

- risques (juridiques, réputation, financiers, etc.) liés à la conformité des systèmes d'encaissement (III.2) ;
- objectifs de conformité de chaque niveau et fonction pour les activités concernées (III.4) ;
- action pertinente pour atteindre les résultats attendus ou prévenir les risques et l'évaluation de son efficacité (III.4) ;
- action pertinente suite à une modification du contexte et/ou du SMC et l'évaluation de son efficacité (III.5) ;
- contrôles de conformité mis en œuvre et leurs résultats (III.6 & III.7) ;
- analyse de la cause d'une NC et des actions prises suite à celle-ci (III.6 & III.7) ;
- processus de conception (III.7) ;
- spécifications fonctionnelles liées à la conformité (III.3 & III.7) ;
- plans de test (III.7) ;
- processus & méthode de développement (III.7) ;
- rapports de test (III.7) ;
- gestion du code source (III.7) ;
- définition du périmètre fiscal (III.7) ;
- gestion de la nomenclature des versions (III.7) ;
- preuve de non impact sur la conformité d'une modification des processus de conception et développement (III.7) ;
- conditions de sous-traitance (III.8) ;
- résultats des processus externalisés (III.8) ;
- identification des fournisseurs/sous-traitants critiques (III.8) ;
- analyse de risques sur la conformité de la sous-traitance (III.8) ;
- action pertinente pour réduction du risque lié à la sous-traitance (III.8) ;
- registre des systèmes et versions distribués (III.9) ;
- informations sur les NC, leur analyse et les actions mises en œuvre (III.13).

Lorsqu'il enregistre et met à jour des informations enregistrées, l'organisme doit s'assurer que les éléments suivants sont définis et corrects :

- identification et description : titre, date, numéro de version du document ;
- format de l'enregistrement (papier, électronique) ;
    - dans le cas d'un enregistrement électronique : nom du fichier et extension (word, pdf, jpg, etc.) ;
- que la revue/approbation du caractère approprié et pertinent des informations est effectuée par les personnes pertinentes avant leur diffusion.

L'organisme doit s'assurer que les documents d'origine externe sont identifiés et empêcher toute utilisation de documents périmés.

Chapitre IV : Exigences techniques applicables au système d'encaissement certifié

Ce chapitre présente les exigences techniques, auxquelles le système d'encaissement certifié doit satisfaire. Le demandeur de la certification est libre de démontrer comment il y répond. Des exemples de solution acceptables sont présentés pour certaines exigences.

Les méthodes de contrôle sont basées sur l'évaluation de la documentation liée au système d'encaissement, des vérifications fonctionnelles et de robustesse sur le système d'encaissement à certifier.

Pour chaque exigence sont décrites, lorsque c'est applicable : l'intitulé de l'exigence, des indications ou exemples de solution(s) acceptable(s) et les modalités de vérification documentaires, fonctionnelles et de robustesse.

IV.1) Documentation

La documentation du système d'encaissement doit décrire l'ensemble des fonctionnalités et mécanismes mis en œuvre dans le cadre de la certification permettant de répondre à l'ensemble des exigences techniques définies dans le présent chapitre. L'organisation de cette documentation doit être décrite dans un document chapeau[17].

L'ensemble de cette documentation doit être :

- conservée sur support papier ou informatique ;
- conservée jusqu'à l'expiration de la 3e année suivant celle au cours de laquelle le système a cessé d'être diffusé[18] ;
- identifiée de façon claire et unique :
    - titre pertinent, en anglais ou en français ;
    - numéro de version du document et/ou date d'approbation du document.

Note : Il est rappelé, pour chaque exigence technique, la documentation attendue dans la case « vérification documentaire ».

Le demandeur de la certification est libre de répondre à chacune de ces exigences dans la documentation règlementaire ou dans la documentation complémentaire tout en respectant les contraintes de celles-ci (langues de rédaction notamment).

[17] CF : IV.1) Exigence 2.
[18] CF : III.10) communication avec les clients

Exigence 1 : documentation règlementaire[19]

Le système d'encaissement doit faire l'objet d'une documentation décrivant sa conception, son exploitation, sa maintenance et son utilisation.

Les documents listés ci-dessous sont visés par le droit de communication de l'administration fiscale, ils doivent être rédigés en français, séparément et intitulés comme suit :

- Dossier de conception générale,
- Dossier de spécifications fonctionnelles,
- Dossier d'architecture technique,
- Dossier organisationnel,
- Dossier de maintenance,
- Dossier d'exploitation,
- Dossier utilisateur

Indications concernant les éléments attendus :

Ces indications ne sont pas exhaustives, leur seul but est d'avoir une meilleure compréhension des attendus de chaque document.

Dossier de conception générale : Décrit le système et ses grands principes de fonctionnement dans leur ensemble, le matériel associé au système pour permettre l'encaissement. Cartographie des différents modules et de leurs interactions. Quels sont les OS et langages utilisés, les caractéristiques du réseau, description succincte des bases de données éventuelles et de la manière dont elles sont interfacées (modèles conceptuels & logiques de données : MCD/MLD). Doit également permettre d'identifier de façon non ambigüe le système : périmètre fiscal, versions mineures/majeures.

Dossier de spécifications fonctionnelles : Description des cas d'usage identifiés, des points d'attention et demandes particulières inhérents au système, définis pendant la phase de conception afin de valider que la solution répondra bien à des besoins expressément identifiés. On doit notamment retrouver les spécifications liées aux exigences du référentiel LNE.

Dossier d'architecture technique: décrit en profondeur l'implémentation technique de la solution : technologies, algorithmes (notamment de signature et hashs utilisés pour la sécurisation des données), frameworks, protocoles utilisés ; architecture détaillée du système (schéma avec nature des flux et les différents composants du système); modalités de sauvegarde etc. Ce dossier doit couvrir tous les traitements effectués sur les données à sécuriser, notamment leur transport, sauvegarde, export, impression et affichage.

Dossier organisationnel : Décrit quels sont les processus et l'organisation mis en place pour la conception, le développement, la configuration / déploiement du système ? RACI, organigrammes etc.

Dossier de maintenance : destiné à identifier le suivi des évolutions/corrections du produit, les processus et l'organisation en place pour la gestion des vulnérabilités, la gestion des licences, les méthodes de mises à jour d'une version (corrective ou évolutive) et de sa livraison chez le client, politique de versionning du code mentionnant la gestion des versions majeures/mineures au sens de la règlementation.

Description de l'architecture du code source (organisation des différents fichiers de code, branches sur le gestionnaire de code) et identification des portions concernées par la certification entrant dans le périmètre fiscal.

Politique de gestion de versions du code (si applicable l'outil utilisé : git, SVN, etc.) identifiant les portions de code impactant le périmètre fiscal, lié aux fonctions de sécurisation, de conservation, d'inaltérabilité et d'archivage au sens du BOI TVA 30-10-30. Ce code, dit « version majeure » ou périmètre majeur/fiscal ne peut faire l'objet de modification sans information du LNE et dans ce cas il fera l'objet d'une évaluation supplémentaire afin d'en vérifier l'impact sur la conformité.

Dossier d'exploitation : Description des configurations et paramétrages possibles du système, de son installation, des prérequis matériels, des modalités de sauvegarde des données, de la gestion des droits utilisateur, de l'utilisation et de la supervision du système par le ou les administrateurs du système ainsi que le remplacement du système.

Dossier utilisateur :

- Manuel utilisateur à destination de l'utilisateur final décrivant les fonctionnalités du système, son mode d'emploi.
- Manuel utilisateur à destination de l'administration fiscale décrivant précisément et simplement l'accès aux données dédié à l'administration fiscale (avec description des éventuels champs de tables, fichiers XML, CSV, etc.) Il peut être inclus dans le manuel utilisateur ou séparé.

Vérification documentaire :

Vérifier que la documentation règlementaire existe, est correctement identifiée (titres, n° de version et/ou date d'approbation) et est bien rédigée en français.

Vérification fonctionnelle :

Vérifier qu'un échantillon de documents relatifs à un système en cours de diffusion est disponible.

Vérification de robustesse :

Vérifier que la documentation technique des méthodes de sécurisation est cohérente avec ce qui est implémenté.

[19] BOI-CF-COM-10-80-20160803 : point 200.

Exigence 2 : documentation complémentaire
La documentation complémentaire est composée de toute la documentation permettant de répondre aux exigences techniques du présent référentiel et ne faisant pas partie de la documentation règlementaire. Elle doit être rédigée en français ou en anglais. L'organisme doit fournir un document chapeau décrivant l'organisation de la documentation et récapitulant pour chaque exigence technique quels sont les documents, les paragraphes et les numéros de page concernés.
Vérification documentaire : Vérifier que la documentation complémentaire est correctement identifiée (titres, n° de version et date d'approbation) et est bien rédigée en français ou en anglais.
Vérification fonctionnelle : Vérifier qu'un échantillon de documents relatifs à un système en cours de diffusion est disponible.
Vérification de robustesse : Vérifier que la documentation technique des méthodes de sécurisation est cohérente avec ce qui est implémenté.

IV.2) Enregistrement des données

Exigence 3 : Données à enregistrer[20]
Le système d'encaissement doit enregistrer toutes les données d'encaissement liées à la réalisation d'une transaction et à son règlement. Ces données doivent être enregistrées au plus tard au moment du calcul du montant total de la transaction avant paiement. Ces données comprennent a minima : - le numéro de justificatif (de transaction le cas échéant), - l'identifiant du TPV[21], - un identifiant unique de l'établissement d'utilisation du système d'encaissement, - la date et l'heure de la transaction (année, mois, jour, heure, minute), - le montant total TTC, - toute donnée permettant la production de justificatifs (définitifs ou provisoires), - le mode de règlement (et les détails des montants réglés par mode de paiement si le règlement a lieu via plusieurs modes de paiement), - la date de règlement (si différente de la date de transaction), - les détails des articles ou prestations : libellé, quantité, prix unitaire, total HT de la ligne, taux de TVA associé. Ces détails doivent inclure toute autre donnée élémentaire[22] nécessaire au calcul du total HT de la ligne. - toute donnée permettant d'assurer la traçabilité de la transaction et de garantir l'intégrité des données d'encaissement

[20] BOI-TVA-DECLA-30-10-30-20180704 : point 50-75-130

[21] TPV : Terminal Point de Vente identifié par un numéro unique (n° de terminal, de caisse, de balance, etc.). Un terminal assure l'enregistrement des données d'encaissement localement, temporairement (en attendant le transfert des données vers un système centralisateur) ou dans le respect avec l'exigence n° 16 concernant la conservation des données pendant la durée de 6 ans à partir de la date de la dernière transaction enregistrée sur l'exercice fiscal courant.

[22] Donnée élémentaire : donnée qui n'est pas obtenue par calcul à partir d'autres données

Exigence 3 : Données à enregistrer[20]
Note spécifique :
Toute référence future aux « données d'encaissement » correspond aux données requises dans cette exigence plus celles générées par les corrections (exigence n°4), celles requises pour l'exigence 5 relative au mode école/test ainsi que les données cumulatives et récapitulatives requises pour l'exigence 7.
Exemples de solutions acceptables :
L'identifiant unique de l'établissement d'utilisation peut être le n° de SIRET de l'établissement ou les coordonnées de l'établissement (adresse complète).
Vérification documentaire :
Description de la méthode utilisée pour enregistrer toutes les données de manière exhaustive.
Vérification fonctionnelle :
Réaliser un ensemble échantillonné d'opérations. Vérifier que l'ensemble des opérations réalisées préalablement apparait dans les données enregistrées. Les cas de test suivants sont à réaliser s'ils sont possibles : application des remises, application des promotions, application des avantages fidélités ou équivalent, réimpressions de ticket, etc.

Exigence 4 : corrections[23]
Si des corrections (modifications ou annulations) sont apportées à des transactions, par quelque moyen que ce soit, ces corrections s'effectuent par un enregistrement des données d'encaissement correctives par le biais d'opérations de « plus » et de « moins », et non par modification directe des données d'encaissement enregistrées.
Vérification documentaire :
Vérifier à partir de la description complète des méthodes de correction des transactions comment la donnée modifiée est liée à la donnée originale et que la traçabilité des modifications est assurée.
Vérification fonctionnelle :
Tester le fonctionnement du système pour vérifier que les corrections s'effectuent par des opérations de "plus" et de "moins" et non par des modifications directes des données d'origines enregistrées. Vérifier par examen de la base de données ou du fichier que les données sont effectivement enregistrées, en cas de correction. Des cas de test doivent inclure les cas suivants : modification de quantité, suppression d'un article, suppression d'un ticket, ajout d'un article à un ticket déjà finalisé avant paiement, application des remises, application des promotions, application des avantages fidélités ou équivalent, etc.

[23] BOI-TVA-DECLA-30-10-30-20180704 : point 90 & 100.

Exigence 5 : Mode école-test[24]

1) Les données générées, ou simulées, par le biais d'un mode ou environnement « école », « test », « recette », « pre-prod » ou autre, permettant l'enregistrement de transactions fictives, doivent être enregistrées et sécurisées comme des données d'encaissement mais explicitement identifiées comme étant issues de ce mode.
2) L'identifiant du responsable de l'opérateur enregistrant les transactions, ainsi que toutes les opérations enregistrées lors de l'utilisation de ce mode/environnement font partie des données d'encaissement. A ce titre ces données doivent respecter toutes les exigences qui les concernent (enregistrement, sécurisation, archivage).
3) Toute pièce justificative émise lors de l'utilisation de ce mode doit être identifiée comme telle en y apposant en trame de fond la mention « factice », « simulation » ou toute autre mention pertinente.
4) L'utilisation du mode école doit être visible depuis l'affichage du système d'encaissement.
5) Si aucun mode de ce type n'est présent dans le système ceci doit être indiqué dans la documentation.

Exemples de solutions acceptables :

Afin d'identifier les données d'encaissement générées par des simulations de transactions, il est par exemple possible d'utiliser un champ spécifique en base de données ou une base de données différente des données de production, à condition que les mêmes mécanismes de sécurisation interviennent et que ces données soient bien intégrées dans les archives.

Vérification documentaire :

Vérifier à partir de la description complète du mode concerné que :

- les données générées sont bien enregistrées et sécurisées comme toute donnée d'encaissement,
- l'identifiant du responsable et toutes les opérations effectuées sont bien enregistrées et sécurisées,
- les données d'encaissement fictives font l'objet d'une identification claire,
- les pièces justificatives font l'objet d'une identification claire,
- l'affichage du système identifie le mode de façon appropriée.

Vérifier que si aucun mode ou environnement ne permet de simuler ou générer des données liées à une transaction fictive, ceci est explicite et argumenté le cas échéant dans la documentation.

Vérification fonctionnelle :

Entrer dans le mode "école" ou "test" ou similaire.

Vérifier dans la base de données et sur les pièces justificatives émises que le fonctionnement est conforme à l'exigence et est cohérent avec la documentation.

Vérifier que les données permettant d'identifier l'usage de ce mode école sont bien sécurisées en essayant de les modifier.

[24] BOI-TVA-DECLA-30-10-30-20180704 : point 90 & 150.

IV.3) Clôtures

Exigence 6 : clôtures annuelles, mensuelles et journalières[26]
Le système d'encaissement doit prévoir des fonctionnalités de clôture journalières, mensuelles et annuelles. Le système d'encaissement ne doit pas permettre d'enregistrer de nouvelles transactions, de modifier ou d'annuler une transaction sur une période clôturée. Ces clôtures peuvent être réalisées automatiquement par le système d'encaissement ou faites par l'utilisateur. Si la clôture doit être réalisée par l'utilisateur, celui-ci doit être informé de cette possibilité.
Note spécifique : Dans le cas de la clôture réalisée par l'utilisateur, il reste de la responsabilité de l'utilisateur du système d'encaissement de réaliser les clôtures périodiques. La clôture annuelle peut se baser sur l'exercice fiscal lorsque celui-ci ne coïncide pas avec l'année civile.
Exemples de solutions acceptables : Il est possible d'avertir l'utilisateur de la nécessité de réaliser les clôtures par tout moyen adéquat (affichage sur l'interface du système, notice d'utilisation, contrat, etc.).
Vérification documentaire : Vérifier à partir de la description de la fonctionnalité de clôture - si les 3 fonctions de clôture (journalière, mensuelle et annuelle) sont bien présentes, - que la fonctionnalité est conforme aux exigences, - que si la fonctionnalité n'est pas automatique l'utilisateur est averti de l'obligation qui lui incombe de réaliser les clôtures.
Vérification fonctionnelle : Enregistrer des transactions et réaliser les clôtures (au moins 1 clôture de chaque niveau) et vérifier la bonne génération des clôtures. Vérifier également qu'il est impossible d'enregistrer une nouvelle transaction ou de modifier/annuler une transaction sur la période clôturée.

Exigence 7 : Données cumulatives et récapitulatives[25]
Pour chaque clôture, le système d'encaissement doit enregistrer le total cumulatif de la période et le total perpétuel comme toute autre donnée d'encaissement.
Note spécifique : Le total cumulatif de la période est le cumul du chiffre d'affaire décompté depuis l'ouverture de la période concernée. Il s'agit d'un compteur initialisé à 0 à l'ouverture de la période (journalière, mensuelle ou annuelle) et dont la valeur est stockée à la clôture. Le total perpétuel est le cumul de chiffre d'affaire décompté depuis le début de l'utilisation du système d'encaissement. Il s'agit d'un compteur ne se remettant jamais à 0 et dont la valeur est stockée périodiquement à chaque clôture. En cas de changement de système d'encaissement tous les compteurs repartent de zéro. Les compteurs de l'ancien système doivent alors être archivés (CF exigence n°10). Dans le cas d'une mise à jour du système, tous les compteurs doivent continuer à être incrémentés sans être remis à 0.
Vérification documentaire : Vérifier à partir de la description des données cumulatives et récapitulatives que la méthode de calcul de ces totaux se base sur le chiffre d'affaire et que ces données sont bien enregistrées pour chaque clôture.
Vérification fonctionnelle : Vérifier sur la base d'un échantillon de données de test représentatives que le système d'encaissement calcule correctement et enregistre bien les totaux cumulatifs de période et total perpétuel pour chacune des périodicités de clôture.
Vérification de robustesse : Vérifier que l'intégrité et l'authenticité des données cumulatives et récapitulatives repose sur un mécanisme robuste.

IV.4) Sécurisation & Inaltérabilité des données

Exigence 8 : Inaltérabilité des données[26]
Toutes les données d'encaissement définies dans les exigences précédentes[27] doivent être conservées de façon inaltérable.
Note spécifique : L'inaltérabilité des données vise à permettre de garantir et d'être en capacité de démontrer par tout procédé technique fiable, l'absence de perte d'intégrité des données d'encaissement et ce depuis leur enregistrement initial. Ce procédé technique doit permettre de détecter et mettre en évidence toute modification ou suppression de données d'encaissement.

[25] BOI-TVA-DECLA-30-10-30-20180704 : point 170.

[26] BOI-TVA-DECLA-30-10-30-20180704 : point 80 & 100.

[27] Définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7, les données de traçabilité des impressions/réimpressions de justificatifs (exigence n°9) ainsi que des opérations de purge, archivage, restaurations des données (exigence n°15)

Exigence 8 : Inaltérabilité des données[26]

Exemples de solutions acceptables :

L'inaltérabilité des données peut être garantie par :

1) la preuve de l'authenticité et de l'intégrité des données qui peut être un chainage d'empreintes à clé, ou un chainage des signatures de chaque enregistrement.
   L'authentification et l'intégrité peuvent être garanties par un mécanisme de signature (tels que RSA-SSA-PSS, ECDSA) ou un mécanisme d'empreinte avec clé (HMAC). La clé doit être générée aléatoirement par un procédé fiable et l'utilisateur final (le professionnel assujetti) ne doit pas pouvoir en avoir connaissance ou être aisément devinable. La signature (ou l'empreinte avec clé) d'une transaction doit inclure des éléments authentifiant la transaction précédente ainsi que la dernière transaction enregistrée (via un compteur ou tout autre élément unique) pour garantir qu'aucune transaction n'ait été supprimée.
   Les exemples de mécanismes d'empreinte à clé suivants sont acceptables : HMAC-SHA-256, HMAC-SHA3.
   Les exemples de fonctions de hachage suivants sont non acceptables : SHA-1, MD5, CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques y compris un CRC32 d'une empreinte SHA256.
   Les exemples d'algorithmes de signatures de données suivant sont acceptables : RSA-SSA-PSS, ECDSA. Pour l'algorithme RSA, il est nécessaire d'utiliser une clé d'au minimum 1024 bits. Il est recommandé d'utiliser une clé de 2048 bits ou plus. Pour les courbes elliptiques, leur ordre doit être d'au moins 256 bits. Les exemples de courbes elliptiques suivantes sont acceptables : ed25519, Brainpool, P-256, ed448.

2) La signature ou la prise d'une empreinte à clé de l'ensemble des données enregistrées. Dans ce cas, à chaque transaction, la nouvelle signature ou l'empreinte à clé doit être calculée sur l'ensemble des données après leur vérification avec l'ancienne valeur.

3) Une parfaite maitrise de l'accès en écriture des données peut être acceptable. Le professionnel assujetti ne doit en aucun cas pouvoir obtenir un accès en écriture aux données. Il est possible que le système s'appuie sur une base de donnée chiffrée et signée (par exemple, avec le mécanisme « encryption at rest » sous Mongodb) pour laquelle la clé cryptographique n'est pas aisément accessible par l'utilisateur (emploi de principes d'enfouissement de clés par exemple, ou de dongle USB externe avec mécanisme de type protection de licence).

Quelle que soit la solution choisie, dans le cas d'un système d'encaissement déployé sur un poste pour lequel l'utilisateur dispose des droits administrateurs il est nécessaire de se prémunir d'une restauration des données dans un état antérieur. L'opération doit être détectée ou rendue impossible. Il est possible d'enregistrer, hors d'accès de l'utilisateur du système d'encaissement, la preuve d'intégrité (signature, empreinte à clé) du dernier enregistrement (dans le cas d'un chainage des données) ou de l'ensemble de la base si le système le permet.

Ces solutions ne sont pas exhaustives et peuvent être utilisées conjointement, d'autres solutions peuvent être acceptées.

Vérification documentaire :

Vérifier que les mécanismes assurant l'inaltérabilité des données sont décrits précisément, incluant les algorithmes de cryptographie utilisés. Vérifier que les données concernées par ces mécanismes comprennent bien l'ensemble des données d'encaissement à sécuriser :

1) toutes les données d'encaissement définies à l'exigence 3,
2) toutes les données correctives définies à l'exigence 4,
3) toutes les données du mode école-test définies à l'exigence 5
4) les données cumulatives et récapitulatives définies à l'exigence 7
5) Les données de traçabilité d'impression/réimpression définies à l'exigence 9
6) Les données de traçabilité des opérations de purge, archivage et restauration des

Exigence 8 : Inaltérabilité des données[26]
données définies à l'exigence n°15.
Vérification fonctionnelle : Vérifier la présence d'un moyen de contrôle de l'intégrité des données ainsi que son efficacité en les modifiant directement sur disque ou en base des données d'encaissement.
Vérification de robustesse : - Réaliser un ensemble d'opérations d'encaissement. - Se connecter sur le dispositif avec l'ensemble des moyens d'accès autorisés, et essayer de modifier les données d'opérations déjà enregistrées. - Vérifier, notamment par un audit de code, que les données d'encaissement enregistrées sont protégées contre leur altération (modification, insertion, suppression ou remplacement) en : o cas 1) : Vérifier que le secret (la clé) est généré de façon aléatoire et qu'il n'est pas accessible par un attaquant. Vérifier que chaque enregistrement est cryptographiquement lié à l'enregistrement qui le précède chronologiquement, en incluant dans le calcul de l'empreinte cryptographique de l'enregistrement courant des éléments authentifiant l'enregistrement précédent, ainsi que la date et l'heure. Vérifier que l'algorithme de signature ou d'empreinte à clé est conforme. Vérifier sur le dispositif, et par échantillonnage, la cohérence d'une chaîne pour un ensemble d'enregistrements contenant des corrections (modifications et des annulations). Vérifier la sécurité des éléments en bout de chaîne, notamment contre leur suppression. o cas 2) : Vérifier que le secret (la clé) est généré de façon aléatoire et qu'il n'est pas accessible par un attaquant. Vérifier qu'à chaque enregistrement, la précédente signature de l'ensemble des données est vérifiée avant son écrasement. o cas 3) : Vérifier que les moyens de protection apportant le même niveau de sécurisation que les exemples précédents sont bien mis en œuvre. Dans le cas d'une maitrise se basant sur un tiers de confiance vérifier les dispositions et SLA prises concernant ces moyens de protection à partir des contrats, termes et conditions, descriptifs de la gestion des droits et du contrôle d'accès, des RACI des équipes intervenant sur les données, des preuves de traçabilité des opérations de maintenance ainsi que de tout autre document jugé pertinent. - Réaliser une analyse de robustesse sur le mécanisme assurant la sécurisation des enregistrements (exemples de tests à réaliser : validation de la chaîne des certificats électroniques, utilisation et implémentation correctes des mécanismes cryptographiques employés et conformité vis-à-vis de l'état de l'art, etc.). - Vérifier que la sécurité des flux de données repose sur des canaux sécurisés (par exemple HTTPS/TLS). - Vérifier que la restauration d'une base ou d'un dossier contenant les données protégées est empêchée ou détectée. - Vérifier que toutes les données d'encaissement concernées par les exigences 3, 4, 5, 7 et 15 sont couvertes par les mécanismes de sécurité. - Conclure sur la capacité du système à garantir l'intégrité et l'authenticité des données.

Exigence 9 : sécurisation des justificatifs
Le système d'encaissement doit permettre de distinguer et identifier sans ambiguïté les justificatifs émis avant paiement des justificatifs émis après paiement. Tout justificatif réimprimé doit porter la mention « duplicata ». Le système doit assurer la traçabilité des impressions et réimpressions de justificatifs (définitifs ou provisoires) de manière sécurisée. Les informations présentes sur les justificatifs doivent être cohérentes avec les données d'encaissement enregistrées par le système d'encaissement.
Note spécifique : Facture, note, reçu, ticket, billets sont des justificatifs.
Exemples de solutions acceptables : Il est possible de faire apparaitre une mention « valable pour encaissement », « provisoire », « pro-forma », « non payé » sur le justificatif avant encaissement et faire apparaitre une mention « paiement réalisé », « paiement reçu », sur le justificatif de reçu d'encaissement. Dans les cas où une même note est partagée entre plusieurs clients, il est possible d'émettre un premier justificatif identifié comme provisoire, puis d'émettre des justificatifs après paiement dont la somme des totaux correspond au total du justificatif provisoire. Il possible d'assurer la traçabilité des impressions/réimpressions de justificatifs en enregistrant et en sécurisant le nombre de d'impressions de chaque justificatif ou de tracer chaque impression/réimpression en enregistrant la date, l'heure et le n° du justificatif (ou de la transaction le cas échéant) dans un journal de logs/d'évènements sécurisé avec le même niveau de sécurité que celui défini à l'exigence n°8.
Vérification documentaire Vérifier à partir de la description des méthodes d'impression des justificatifs que toutes les exigences sont prévues et documentées.
Vérification fonctionnelle Vérifier suivant les différents cas d'usage du système la cohérence des justificatifs émis avec les transactions enregistrées ainsi que la mise à jour des compteurs d'impression en base. Vérifier dans les cas de partage d'addition/note que la somme des montants des différents justificatifs est bien égale au montant TTC de la transaction initiale.

IV.5) Archivage des données d'encaissement

Exigence 10 : Archivage des données
Le système d'encaissement doit prévoir une fonctionnalité d'archivage, à destination des utilisateurs, permettant l'export dans un format ouvert[28], des données d'encaissement[29] figées et horodatées. En cas de changement de système d'encaissement les données cumulatives et récapitulatives[30] doivent être archivées.

[28] Format ouvert : format de données interopérable, c'est-à-dire indépendant du logiciel utilisé pour le créer, le modifier ou le lire, et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre. *Art 4 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*

[29] Définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7, les données de traçabilité d'impression/réimpression de justificatifs définies dans l'exigence n°9, les données de traçabilité des opérations de purge et d'archivage, les données de traçabilité de la remontée des données des TPV vers le système centralisateur le cas échéant.

[30] CF exigence n°7

Exigence 10 : Archivage des données
Note spécifique La fonctionnalité d'archivage ne doit pas être confondue avec seulement une solution de sauvegarde à long terme des données. Il s'agit bien d'exporter du système, dans un format ouvert, les données d'encaissement figées, horodatées et sécurisées afin de se prémunir d'une perte des données suite à un problème matériel, une faille de sécurité, un changement de système d'encaissement ou tout autre raison. Il s'agit d'un moyen pour l'assujetti de pouvoir conserver indépendamment du système d'encaissement ses données d'encaissement et pouvoir les communiquer à l'administration fiscale en cas de contrôle. Il n'est pas de la responsabilité de l'éditeur du système d'encaissement de réaliser l'archivage. Par contre, le système doit permettre à son utilisateur d'archiver les données. La réalisation de l'exécution de l'archivage reste de la responsabilité de l'utilisateur du système.
Exemple de solutions acceptables : Les formats pour les données d'archivage suivants sont des formats ouverts acceptables: ods, xlsx, odb, csv, json, xml, txt. Si les données d'archivage sont compressées, les formats de compression suivants sont des formats ouverts acceptables : Zip, 7z, gz, bz2, tar, rar. A contrario les formats suivants sont des formats fermés ou propriétaires non acceptables : xls, mdb.
Vérification documentaire Vérifier, à partir de la description de la fonctionnalité d'archivage que celle-ci est existante, qu'un utilisateur du système d'encaissement peut l'utiliser et en est averti, que le format est ouvert et que les données présentes dans l'archive sont bien figées, horodatées et complètes. Vérifier, si nécessaire, la présence d'un engagement de l'éditeur du système d'encaissement, à fournir, aux utilisateurs, ainsi qu'à l'administration fiscale, les données d'archivage, notamment dans le cas où l'utilisateur cesse d'utiliser le système d'encaissement.
Vérification fonctionnelle Vérifier la disponibilité de la fonctionnalité d'archivage, que celle-ci fournit bien des archives dans un format ouvert et que les données présentes sont bien horodatées et complètes. Vérifier qu'il est possible d'archiver les totaux cumulatifs de période et totaux perpétuels figés à chaque période.
Vérification de robustesse Vérifier que l'intégrité et l'authenticité des données de la date de création de l'archive est protégée par un mécanisme robuste, tel que décrit à l'exigence n°8.

Exigence 11 : Périodicité d'archivage
Cette fonctionnalité d'archivage doit permettre à l'utilisateur, à toute date, d'avoir accès ou de pouvoir générer les archives pour toute période passée. La période couverte par une archive ne doit pas pouvoir être supérieure à un an ou à un exercice fiscal.
Exemples de solutions acceptables Il est acceptable de donner à l'utilisateur la possibilité de définir les bornes de la période dont il souhaite réaliser l'archivage (tout en respectant la contrainte maximale d'une année/exercice) ou de générer plusieurs fichiers d'archive périodiques (journalières, mensuelles et/ou annuelles).
Vérification documentaire Vérifier, à partir de la description de la fonctionnalité d'archivage que l'utilisateur a la possibilité d'archiver toute période souhaitée sans toutefois pouvoir dépasser un an ou un exercice fiscal par archive.
Vérification fonctionnelle Vérifier que l'utilisateur peut archiver toutes les données d'encaissement pour toute période souhaitée (en un ou plusieurs fichiers), à toute date, sans toutefois pouvoir dépasser la limitation d'un an/exercice par archive. Réaliser par exemple une ou des archives pour une période de plusieurs jours, 1 mois, plusieurs mois et/ou 1 an. Vérifier qu'il est impossible de faire un fichier d'archive dépassant une période d'un an ou d'un exercice fiscal.

Exigence 12 : Intégrité des archives
Les données contenues dans l'archive doivent être conformes aux données initiales figées à partir desquelles elle a été créée et doit prévoir un mécanisme fiable, indépendant du support de conservation de l'archive, garantissant cette intégrité et permettant de la vérifier.
Note spécifique Ces mécanismes doivent permettre de détecter et mettre en évidence toute modification ou suppression de données d'encaissement conservées dans l'archive. Ils doivent aussi permettre de détecter et mettre en évidence toute différence avec la donnée d'encaissement initialement enregistrée ainsi que la date d'encaissement contenue dans l'archive. Le niveau de sécurité de ces mécanismes doit être au moins équivalent à celui utilisé pour répondre à l'exigence 8.
Exemples de solutions acceptables A titre d'exemple, un support externe sécurisé de type disque dur externe chiffré est envisageable. Une alternative peut être la production d'une archive sécurisée (par signature ou empreinte à clé) qui est stockée sur un dispositif externe (disque externe, clé USB, etc.). Dans le cas d'un support externe non sécurisé, c'est l'archive qui doit être sécurisée. La conservation des archives dans le cloud est possible dans le respect des règles de l'art.
Vérification documentaire Vérifier que les mécanismes assurant l'intégrité des archives sont décrits précisément, incluant les algorithmes de cryptographie utilisés.
Vérification fonctionnelle Vérifier la présence d'un moyen de contrôle de l'intégrité des archives ainsi que son efficacité en essayant de modifier directement l'archive.
Vérification de robustesse Vérifier que l'inaltérabilité des archives dans le temps repose sur un mécanisme robuste, garantissant un niveau de protection au moins équivalant à celui demandé à l'exigence n°8. Vérifier l'existence et la fiabilité d'un mécanisme de vérification de l'intégrité des archives indépendant du support de stockage.

IV.6) Purges

Exigence 13 : Purge[31]
Si le système d'encaissement dispose d'une fonctionnalité de purge des données d'encaissement, liée à la nécessité de libérer de l'espace mémoire, il doit garantir avant la mise en œuvre de la purge, la génération d'une archive contenant toutes les données d'encaissement à purger et sa conservation conformément à l'exigence n°17.
Vérification documentaire Vérifier à partir de la description de la méthode de purge que celle-ci est systématiquement précédée de la génération d'une archive contenant bien toutes les données d'encaissement à purger. Si aucune procédure de purge n'existe, vérifier que ceci est bien décrit dans la documentation.
Vérification fonctionnelle Créer une archive fictive initiale contenant un échantillon de données d'origines et de modification, copier cette archive sur un autre support puis mettre en œuvre la procédure de purge. Vérifier la complétude de l'archive générée par la purge par rapport à l'archive initiale.
Vérification de robustesse Vérifier que l'archive générée par ce biais est sécurisée avec le même niveau qu'à l'exigence n°12. Créer une archive sur une période déterminée. Effectuer une purge des données de cette même période. Vérifier que l'archive est bien cohérente.

Exigence 14 : Purge partielle[32]
La fonctionnalité de purge ne doit pas supprimer du système d'encaissement les données cumulatives et récapitulatives[33] ainsi que les données de traçabilité des opérations[34]. Celles-ci doivent rester indéfiniment conservées[35], sécurisées[36], dans le système d'encaissement.
Vérification documentaire Vérifier à partir de la description de la méthode de purge que les données cumulatives, récapitulatives et de traçabilité sont toujours correctement conservées, sécurisées dans le système d'encaissement lui-même.
Vérification fonctionnelle Sur un système de caisse représentatif, introduire des données connues, réaliser une purge et vérifier l'exactitude, et la bonne conservation, des données cumulatives et récapitulatives pour la période dont les données ont été purgées, contenues dans le système d'encaissement en les comparant avec les données initialement introduites.
Vérification de robustesse Vérifier que le mécanisme de purge ne remet pas en cause l'intégrité des données cumulatives et récapitulatives conservées dans le système d'encaissement pour la période dont les données ont été purgées.

[31] BOI-TVA-DECLA-30-10-30-20180704 : point 250.
[32] BOI-TVA-DECLA-30-10-30-20180704 : point 260.
[33] CF exigence n°7
[34] CF exigence n°15
[35] CF exigence n°17
[36] CF exigence n°8

IV.7) Traçabilité des opérations

Exigence 15 : Traçabilité des opérations
Le système d'encaissement doit assurer de manière sécurisée la traçabilité des opérations d'archivage, de purge, de restauration des données en enregistrant, dans le système, pour chacune de ces opérations son horodatage et l'identifiant du TPV depuis lequel l'opération est faite.
Exemples de solutions acceptables Il est possible que la traçabilité de ces opérations soit assurée par un journal d'évènements ou de logs sécurisé selon le même niveau que défini dans l'exigence 8.
Vérification documentaire Vérifier à partir de la description des moyens d'assurer la traçabilité de ces opérations que toutes les clôtures, purges et générations d'archive sont concernées par le mécanisme.
Vérification fonctionnelle Après avoir réalisé un ensemble d'opérations d'archivage vérifier sur le système: - qu'il est possible de recenser l'ensemble des opérations d'archivage réalisées ; - qu'un horodatage des archives est mis en place ; - qu'une association existe entre l'archive et le dispositif qui a produit l'archive. - qu'une modification d'une donnée de traçabilité est détectée par le système.
Vérification de robustesse Vérifier que les mécanismes de sécurisation des données de traçabilité mis en œuvre sont au moins équivalents en termes de niveau de sécurité que celui atteint dans l'exigence n°8. Vérifier que l'horodatage des opérations repose bien sur un mécanisme fiable et qu'il n'est pas possible de le modifier.

IV.8) Conservation des données

Exigence 16 : Conservation des données
Toutes les données d'encaissement, de traçabilité, ainsi que les preuves de leur inaltérabilité, doivent être conservées pendant 6 ans (à compter de la date de la dernière opération de l'exercice fiscal)[37]. Les données cumulatives et récapitulatives ainsi que les données de traçabilité[38] doivent être conservées dans le système[39]. Les données d'encaissement (hors données cumulatives et récapitulatives et les données de traçabilité) peuvent être conservées soit dans le système lui-même soit dans les archives.
Note spécifique Les données d'encaissement concernées sont toutes celles définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5, les données cumulatives et récapitulatives définies dans l'exigence n°7 ainsi que les données de traçabilité définies dans l'exigence 15. Un assujetti ne conservant que le Z de caisse (total cumulatif de la journée) ne respecte pas ses obligations de conservation. Les vérifications concernant la durée de conservation des données se basent une durée de 7 ans afin de simplifier les interprétations possibles du Livre des Procédures Fiscales et prendre en compte les cas exceptionnels de décalage d'exercice fiscal. Le système doit permettre de se prémunir des défaillances matérielles d'un support de stockage ou

[37] CF article L.102 B du Livre des Procédures Fiscales
[38] CF exigence n°15
[39] CF exigence n°14

Exigence 16 : Conservation des données
explicitement prévenir l'utilisateur (assujetti) de sa responsabilité quant à l'obligation de conserver ses données conformément à la présente exigence.
Exemples de solutions acceptables : Il est par exemple possible de mettre en œuvre des processus et/ou des outils de supervision de la capacité mémoire, de faire une estimation de la capacité mémoire nécessaire, d'avertir l'utilisateur de la nécessité de réaliser une purge, augmenter la capacité mémoire si nécessaire ou redonder des sauvegardes sur des supports physiques si possible distants.
Vérification documentaire Vérifier à partir de la description de la méthode de conservation des données d'encaissement que toutes les données d'encaissement sont bien conservées pendant un délai de 7 ans. Vérifier pour les données d'encaissement hors données cumulatives, récapitulatives et de traçabilité si la conservation a bien lieu soit dans le système soit dans les archives. Vérifier que l'éditeur a mis en places des dispositions pour prévenir le risque de saturation mémoire et que le système permet une conservation des données pendant au moins 7 ans.
Vérification fonctionnelle Vérifier que les dispositions mises en place par l'éditeur pour réduire le risque de saturation mémoire fonctionnent efficacement. Vérifier pour les données d'encaissement hors données cumulatives, récapitulatives et de traçabilité si la conservation a bien lieu soit dans le système soit dans les archives. Vérifier que les données cumulatives, récapitulatives et de traçabilité sont bien conservées dans le système lui-même.
Vérification de robustesse Dans le cas où la conservation des données est assurée par le système et non par les archives, vérifier l'aptitude du système d'encaissement à conserver les données d'encaissement pendant une durée de 6 ans. Vérifier que cette aptitude repose, par exemple, sur l'utilisation d'un mécanisme assurant le niveau de disponibilité adéquat au niveau du système de stockage (RAID-1 matériel ou logiciel) ou au niveau du système de fichiers (redondance des fichiers sur plusieurs unités de stockage, journalisation et capacité d'autoréparation, etc.). Vérifier que la configuration des mécanismes mis en œuvre permet de s'assurer la bonne conservation et disponibilité des données d'encaissement pendant 7 ans.

Exigence 17 : Conservation des archives
Les archives doivent être conservées de manière à garantir l'intégrité et la disponibilité des données archivées en cas de contrôle pendant 6 ans (à compter de la date de la dernière opération de l'exercice fiscal).
Exemples de solutions acceptables : Les archives peuvent être conservées, dans le système d'encaissement, en dehors, ou par un tiers archiveur qui se charge d'assurer la conservation des archives. Les mesures nécessaires doivent être prises pour garantir l'intégrité et la disponibilité des archives conformément aux exigences n°12 et 16.
Vérification documentaire Vérifier à partir de la méthode de conservation des archives comment celles-ci sont conservées de façon à garantir leur intégrité et leur disponibilité avec le même niveau de confiance que pour les exigences n°12 et 16.

Vérification fonctionnelle Vérifier comment les archives sont conservées de façon à garantir leur intégrité et leur disponibilité avec le même niveau de confiance que pour les exigences n°12 et 16.
Vérification de robustesse Vérifier l'aptitude du système d'encaissement à conserver les archives intègres et disponibles avec le même niveau de confiance que pour les exigences n°12 et 16.

Exigence 18 : Système centralisateur[40]

Lorsque la conservation des données[41] est assurée sur un système centralisateur, le système d'encaissement doit prévoir des mécanismes fiables démontrant l'exhaustivité et la traçabilité de la remontée des données d'encaissement.

Le système doit prévoir le cas d'une perte de connexion entre le système centralisateur et les terminaux et s'assurer que les TPV ne pourront pas continuer de fonctionner indéfiniment sans connexion avec le système centralisateur.

Note spécifique

Un système est dit centralisateur si un ou des TPV qui assurent localement le stockage de l'information avant transmission (cas des caisses autonomes remontant périodiquement les données ou qui remontent les données en temps réel tout en prévoyant un système de buffer en cas de déconnexion) transmettent les données d'encaissement vers un système central qui en assure la conservation dans le respect de l'exigence n°16.

A contrario un système avec une architecture client-serveur où l'interface client n'est qu'une interface graphique, sans stockage temporaire des données, qui permet la communication vers un serveur (cas d'une application web ouverte dans un navigateur par exemple) n'est pas considéré comme un système centralisateur dans la mesure où l'utilisation autonome de l'interface sans connexion avec le serveur est impossible.

Si la conservation des données dans le respect des exigences n° 8 et 16 est assurée par les terminaux cette exigence est non-applicable.

La traçabilité de la remontée des données d'encaissement vise à s'assurer que l'ensemble des données de transaction sont bien remontées y compris en cas de problèmes de connectivité ou d'erreurs de transmission.

Exemples de solutions acceptables :

Afin de garantir l'exhaustivité du transfert de donnée, il est possible de mettre en place une numérotation incrémentale horodatée des envois et réceptions de données ou une référence au dernier enregistrement envoyé (comme par exemple un hash de l'enregistrement), couplé à une identification du TPV source afin de s'assurer qu'aucune donnée n'est manquante.

Afin de garantir l'intégrité des données transférées, il est possible d'utiliser une signature, une empreinte à clé, ou un protocole réseau sécurisé (comme par exemple TLS, IPsec).

Si le système prévoit que les TPV puissent effectuer des transactions de manière autonome en cas de perte de la connexion avec le système centralisateur, les données stockées localement doivent avoir un niveau de sécurité au moins équivalent à celui apporté en réponse à l'exigence 8. De plus, lors du rétablissement de la connexion, le système centralisateur doit s'assurer avoir récupéré toutes les données stockées localement et temporairement par les TPV.

Vérification documentaire

Si la conservation des données est assurée par les terminaux, vérifier les éléments permettant de démontrer l'inapplicabilité de cette exigence.

Si la conservation des données est assurée par le système centralisateur vérifier à partir de la description complète de ce système que l'exhaustivité de la remontée des données est démontrée et que ces remontées sont tracées. Vérifier que l'éditeur fournit une déclaration explicite d'exhaustivité de la remontée des données d'encaissement.

Vérification fonctionnelle

Si la conservation des données est assurée par les terminaux, vérifier les éléments permettant de démontrer l'inapplicabilité de cette exigence.

Vérifier la bonne traçabilité du système de remontée des données d'encaissement des TPV vers le système centralisateur.

Vérifier la bonne remontée dans le système centralisateur d'un ensemble échantillonné de données d'encaissement.

[40] BOI-TVA-DECLA-30-10-30-20180704 : point 210.

[41] CF exigence n°13

Exigence 18 : Système centralisateur[40]

Vérification de robustesse

Dans le cas de l'utilisation de compteurs traçant le nombre de transactions émises et réceptionnées, réaliser un ensemble d'opérations depuis les TPV reliés au système centralisateur, et vérifier sur ce dernier, qu'à chaque enregistrement réalisé sur un TPV est associé :

l'identifiant du TPV concerné, une numérotation incrémentale traçant le moment de l'envoi des données par le TPV, des numérotations incrémentales traçant l'ensemble des réceptions de données de transaction depuis chaque TPV par le système centralisateur afin de s'assurer qu'un envoi n'a pas été omis.

Dans le cas d'un chiffrement ou d'une signature des envois de données vérifier que le niveau de sécurité est au moins équivalent à celui apporté en réponse à l'exigence n° 8.

Vérifier que l'ensemble des données d'encaissement sont bien stockées et conservées sur le système centralisateur. Vérifier qu'une défaillance dans la transmission des données ou dans la réception des données n'engendre pas un manque ou une donnée erronée dans le système centralisateur.

Vérifier que le mécanisme de protection contre l'altération des envois est d'un niveau de sécurité au moins équivalent à celui permettant de répondre à l'exigence n° 8.

Vérifier qu'en cas de perte de connexion il n'est pas possible d'effectuer indéfiniment des transactions sur les TPV et que le mécanisme est suffisamment robuste pour contrôler que tous les éléments sont bien remontés lors du rétablissement de la connexion.

IV.9) Accès de l'administration fiscale aux données d'encaissement

Exigence 19 : Accès de l'administration fiscale aux données[42]
Le système d'encaissement doit prévoir un accès pour l'administration fiscale à l'ensemble des données d'encaissement[43] enregistrées. L'éditeur doit fournir un moyen automatisé pour que l'administration fiscale puisse vérifier l'intégrité des données d'encaissement. L'éditeur doit fournir un manuel utilisateur à destination de l'administration fiscale, en français, détaillant la procédure permettant d'accéder aux données, ainsi qu'un descriptif clair du fonctionnement des outils utilisés pour accéder aux données et en vérifier l'intégrité. Cet accès ne doit pas remettre en cause la sécurité des données d'encaissement.
Note spécifique : Le manuel utilisateur à destination de l'administration fiscale doit être clair et compréhensible par un non-informaticien. Il doit par ailleurs détailler la procédure permettant de vérifier que les données n'ont pas été altérées.
Exemples de solutions acceptables : Il peut être possible d'exploiter le compte gérant, ou un compte dédié à l'administration, pour accéder à l'ensemble des données de l'entreprise, qui peuvent être sous une forme native (fichiers à plat, fichiers XML, etc.) ou une forme interprétée pour des fins de visualisation. Il est possible de détailler le processus de contact et d'escalade auprès du support si nécessaire dans le manuel à destination de l'administration fiscale. Celui-ci peut être inclus dans le manuel utilisateur ou être un manuel distinct. La structure de la présentation des données (les différents champs) doit être décrite de façon explicite. L'interface utilisateur, les menus, fenêtres et autres fonctionnalités à destination de l'administration fiscale peuvent être décrits dans le manuel à sa destination.
Vérification documentaire Vérifier à partir de la description du moyen d'accès de l'administration fiscale que toutes les données d'encaissement sont accessibles. Vérifier l'existence et la pertinence du manuel à destination de l'administration fiscale décrivant les moyens et procédures permettant l'accès aux données d'encaissement.
Vérification fonctionnelle Vérifier que moyen permettant d'accéder aux données pour l'administration fiscale fonctionne correctement et que toutes les données d'encaissement sont accessibles. Vérifier que ce moyen ne permet pas de modifier ou supprimer des données d'encaissement. Vérifier que le moyen fourni à l'administration fiscale permet la bonne détection de l'altération (modification, insertion, suppression) des données. Par exemple, modifier une donnée et vérifier que la détection de cette erreur est aisée et immédiate en utilisant le moyen d'accès de l'administration fiscale.
Vérification de robustesse Vérifier que les modalités d'accès par l'administration ne remettent pas en cause le niveau de sécurité du système d'encaissement.

[42] BOI-TVA-DECLA-30-10-30-20180704 : point 60 & 100.

[43] Définies dans l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n° 4, les données du mode école-test définies dans l'exigence n° 5, les données cumulatives et récapitulatives définies dans l'exigence n° 7, les données de traçabilité des opérations définies dans l'exigence n° 15 ainsi que les données de traçabilité de la remontée exhaustive des données dans le cas d'un système centralisateur.

IV.10) Identification du périmètre fiscal et des versions majeures et mineures

Exigence 20 : Identification du périmètre fiscal
L'éditeur doit définir clairement le périmètre fiscal de son système d'encaissement et lister de façon exhaustive tous les fichiers du code source, des librairies, pilotes et modules impactant les fonctionnalités et exigences énoncées dans le présent référentiel.
Notes spécifiques : Si une partie du périmètre fiscal est protégé par une configuration spécifique du système d'exploitation, les fichiers de la configuration considérée doivent avoir une identification additionnelle. Le périmètre non fiscal est dit « périmètre mineur ». Le code source du périmètre mineur doit être disponible aux évaluateurs lors de l'évaluation de robustesse afin de vérifier la cohérence de la définition des périmètres fiscal et mineur.
Exemples de solutions acceptables Sont par exemple inclus dans le périmètre fiscal toutes les fonctions d'enregistrement des données d'encaissement ; de correction/annulation d'une transaction ; les fonctions liées à l'enregistrement et à la sécurisation des données générées par le mode école ; les fonctions de clôture (journalière, mensuelle et annuelle) ; de calcul, d'enregistrement et de sécurisation des données cumulatives et récapitulatives ; de sécurisation et d'inaltérabilité des données d'encaissement ; de sécurisation des justificatifs ; d'archivage ; de sécurisation des archives ; de purge ; de traçabilité des opérations (archivage, purges, clôtures) ; de conservation des données et des archives ; d'accès de l'administration fiscale et de toute autre fonctionnalité/module/pilote/librairie impactant le respect des exigences du présent référentiel. Il est possible de définir le périmètre fiscal comme étant l'entièreté du code source du système d'encaissement.
Vérification documentaire Vérifier à partir de la liste des composants du périmètre fiscal que celle-ci est complète afin que l'organisme de certification et l'éditeur n'aient aucun doute sur les portions de code source dont la modification entraine un changement de version majeure.
Vérification de robustesse Vérifier par analyse du code source que l'ensemble des fonctionnalités règlementaires (i.e. en lien avec la certification et les exigences du présent référentiel) sont implémentées dans des fichiers de code source inclus dans le périmètre fiscal. Vérifier par échantillonnage du code source qu'il n'y a pas de fonctionnalités règlementaires dans le périmètre non fiscal (mineur)

Exigence 21 : Identification des versions majeures et mineures

Le système d'encaissement doit être clairement identifié par un numéro de version majeure et un numéro de version mineure inextricablement liés au système d'encaissement.
Ces numéros de version doivent être aisément accessibles depuis l'interface utilisateur standard du système d'encaissement.
Toute modification de code dans le périmètre fiscal ou paramétrage impactant le respect des exigences du présent référentiel doit entrainer une incrémentation du numéro de version majeure.
L'éditeur doit générer et fournir l'empreinte de chaque version majeure.

Note spécifique :

Le numéro de version majeure du système d'encaissement est l'identification du numéro de version du périmètre fiscal du système d'encaissement.
Le numéro de version mineure du système d'encaissement est l'identification du numéro de version du code non inclus dans le périmètre fiscal n'impactant donc pas le respect des exigences du présent référentiel.
Si des fonctions du système d'encaissement peuvent être désactivées par des paramétrages spécifiques, chaque fonction ou variante doit être identifiée séparément.

Exemples de solutions acceptables

Les algorithmes suivants sont à l'état de l'art pour réaliser les empreintes des logiciels ou sous-parties des logiciels dans un but d'identification précise : SHA-2, SHA-3, Whirlpool, Blake.
A contrario les algorithmes suivants sont non acceptables : SHA-1, MD5, CRC16, CRC32 et toutes autres formes de sommes de contrôles non cryptographiques.
Il est possible de faire les empreintes utilisées pour l'identification des versions à partir du binaire ou du code source. L'empreinte peut être stockée à côté du code source.
Dans le cas des systèmes accessibles directement par les clients finaux (e-commerce par exemple), l'affichage du numéro de version du système d'encaissement peut être limité à un profil spécifique (contrôleur fiscal ou administrateur par exemple).

Vérification documentaire

Vérifier à partir de la documentation comment l'identification du système par les numéros de version est créée et comment est inextricablement liée au système lui-même. Vérifier dans la documentation quelles sont les mesures prises pour protéger l'identification du système d'encaissement d'une quelconque falsification.
Vérifier qu'il est décrit dans le manuel utilisateur comment afficher l'identification des versions majeures et mineures du système depuis l'interface utilisateur.
Vérifier que les règles de nomenclature des versions majeures et mineures sont clairement établies et conformes à l'exigence.
Vérifier à partir de la documentation que l'éditeur a fourni le numéro de version majeure et le numéro de version mineure du système d'encaissement évalué lors de l'audit de certification.

Vérification fonctionnelle

Vérifier que l'identification du logiciel est visualisée conformément à sa description dans la documentation. Vérifier que l'identification présentée est correcte.

Vérification de robustesse

Vérifier que le mécanisme permettant de générer l'identification du système via les numéros de version majeure et mineure a intégré toutes les parties du système concernées et que celui-ci est fiable, c'est-à-dire qu'il suit les critères de l'annexe B1 du RGS, ou, a minima, est résistant à une attaque par collision (c'est-à-dire qu'il n'est pas possible de forger deux sources distinctes produisant la même empreinte).
Vérifier que les mesures prises pour éviter la falsification sont appropriées par rapport à l'état de l'art.
Vérifier par échantillonnage à partir du journal des versions (« changelog ») ou au différentiel en termes de code entre deux versions que les modifications mineures n'ont pas d'impact sur le respect des exigences du présent référentiel.

Exigence 21 : Identification des versions majeures et mineures
Vérifier qu'une empreinte réalisée par l'évaluateur sur le code certifié produit la même empreinte que celle délivrée par l'éditeur.

Le certificat porte sur une version majeure du système d'encaissement donnée (et évaluée lors de l'audit de certification) et demeure valable pour attester du respect des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données pour les versions mineures ultérieures à la version mineure évaluée par le LNE au cours de l'évaluation de certification.

Chapitre V : Elaboration et validation du référentiel

V.1) Comité de marque

V.1.1) Modalités de fonctionnement

Il est constitué un comité de marque dont les attributions sont de :

- donner un avis sur les règles de certification et ses évolutions,
- donner un avis sur les projets d'actions de communication ou de promotion relatifs à la marque.

Le comité de marque se réunit au minimum une fois par an en réunion ordinaire. Des comités extraordinaires peuvent être organisés chaque fois que nécessaire (par exemple en vue de modifier les règles de certification).

Préalablement à la réunion du comité, le LNE transmet aux membres du comité, un ordre du jour de la séance accompagné, le cas échéant, des documents associés. Le LNE rédige le compte-rendu des observations et propositions formulées en réunion de comité. Ce compte-rendu est adressé à tous les membres du comité. Le cas échéant, un bureau du comité ou des groupes de travail pourront compléter le dispositif pour gagner en efficacité.

La composition nominative du comité de marque est approuvée par le directeur général du LNE ou son délégué, chaque membre en étant ensuite informé. Le mandat des membres est de 3 ans, il est renouvelable par tacite reconduction.

L'exercice des fonctions de membre du Comité de marque est strictement personnel. Toutefois, en cas d'absence, un suppléant est désigné et nommé dans les mêmes conditions que le titulaire.

V.1.2) Rôle, engagements et composition du comité

Les membres du comité s'engagent à :

- contribuer de par leur expertise au bon fonctionnement de la marque de certification des systèmes de caisse ;
- conserver la confidentialité des échanges et informations communiqués au cours des réunions du comité de marque et ceci jusqu'à leur publication par le LNE ;
- participer régulièrement aux réunions ;
- contribuer au développement de la marque de certification et promouvoir les prestations certifiées.

Le comité est composé comme suit :

- 3 représentants des clients certifiés ou en cours de certification :
  - 1 représentant parmi les éditeurs de logiciel,
  - 1 représentant parmi les fabricants de caisses,
  - 1 représentant parmi les fabricants de dispositifs d'encaissement associés à un instrument de mesure réglementé,
- 2 représentants des associations ou organismes représentatifs des consommateurs et / ou des utilisateurs ou à défaut les utilisateurs eux-mêmes.

Chaque collège dispose d'une voix. Aucune des parties intéressées ne peut faire valoir un droit de veto.

Le LNE assure le secrétariat du comité.

V.1.3) Groupe de travail

Pour la conduite de certains travaux ponctuels, d'ordre technique et ne nécessitant pas la convocation de l'ensemble des membres du comité de marque, il peut être créé un groupe de travail dont les membres sont désignés nominativement et choisis parmi ceux du comité de marque. Dans le cas d'un groupe de travail, il peut être fait appel à des professionnels ou des personnalités extérieures au comité.

Les missions de ce groupe de travail sont précisées par le comité de marque ; ses attributions seront généralement limitées à l'élaboration de projets, de propositions ou à la fourniture de compléments d'information sur un sujet donné pour le compte du comité de marque.

V.2) Modalités d'élaboration et de validation du référentiel

Le présent référentiel a été élaboré par le LNE, à partir des documents de travail issus des réunions du groupe d'experts et du comité, comprenant les fabricants des systèmes de caisse, les éditeurs de logiciel d'encaissement, les donneurs d'ordres, les utilisateurs.

Sa rédaction a été faite conformément aux exigences de la loi du 4 août 2008 et du décret du 19 décembre 2008 régissant la certification des produits et des services. À ce titre et d'après l'article L433-3 et suivants et R433-1 et -2 du code de la consommation, le référentiel de certification est un document technique définissant les caractéristiques que doit présenter un produit, un service ou une combinaison de produits et de services, et les modalités de contrôle de la conformité à ces caractéristiques.

Pour la validation de ce référentiel, le LNE a la responsabilité :

- d'identifier les parties intéressées concernées ;
- de s'assurer de la pertinence des parties intéressées sélectionnées ;
- de s'assurer de leur représentativité, sans prédominance de l'une d'entre elles ;
- de recueillir leur point de vue.

Sur la base du retour d'expérience, le référentiel est passé en revue au sein d'un comité de marque spécifiquement constitué, intégrant l'ensemble des parties intéressées. Son approbation est effectuée selon la même méthodologie que la première version.

V.3) Normes et documents de référence

- Norme NF EN ISO 9001:2015 : Systèmes de management de la qualité – Exigences.
- Norme NF EN ISO 19600:2014 : Systèmes de management de la conformité – Lignes directrices

- Loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016 – Article 88, modifiée par la loi n° 2017-1837 article 105

- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

- Code de la consommation – version du 1er janvier 2019 – articles L433-3 à L433-11, articles R433-1 et R433-2

- Code général des impôts – version du 1er janvier 2019 – articles 286, 1770 duodecies

- Livre des procédures fiscales – version du 1er janvier 2019 – articles L 16-0 BA, L47 A, L80 O, L96 J, L102 B, L102 D

- Arrêté du 29 juillet 2013 portant modification des dispositions de l'article A. 47 A-1 du livre des procédures fiscales relatif aux normes de copies des fichiers sur support informatique

- BOI-TVA-DECLA-30-10-30-20180704 : Obligation d'utilisation de logiciels ou systèmes de caisse certifiés
- BOI-CF-COM-10-80-20160803 : Droit de communication auprès de diverses personnes
- BOI-BIC-DECLA-30-10-20-40-20131213 : Conservation et représentation des livres, documents et pièces comptables dans le cadre d'une comptabilité informatisée
- BOI-CF-IOR-60-40-20131213 : Contrôle des comptabilités informatisées

- Référentiel général de sécurité version 2.0 –Annexe B1 – Mécanismes cryptographiques – version 2.03 du 21 février 2014

Chapitre VI : Recours et traitement des plaintes

VI.1) Recours contre décision

Le titulaire de la certification peut contester la décision prise par courrier avec accusé réception.

Dans un premier temps, le LNE procède au réexamen du dossier au vu des éléments factuels motivant le recours. Il notifie le maintien ou la nouvelle décision au demandeur dans un délai de 15 jours ouvrés à réception du recours.

Dans le cas où le demandeur désire maintenir son recours contre décision, il le notifie au LNE par lettre recommandée avec accusé réception dans un délai de 15 jours ouvrés. Ce recours, non suspensif de la décision du LNE, doit être motivé. Il est instruit par le LNE dans les 21 jours ouvrés suivant sa réception et donne lieu, lorsqu'il concerne la décision de certification, à examen par le comité de lecture. Le LNE informe l'auteur du recours, du maintien ou non de sa décision.

En cas de maintien du recours après instruction et soumission au comité de marque pour avis, le recours est présenté au Comité de Certification et de Préservation de l'Impartialité du LNE, qui après examen, propose ses conclusions. La décision finale est notifiée par le LNE à L'Entreprise.

Toute contestation ultérieure peut être soumise à l'arbitrage de la direction compétente du
Ministère chargé de l'Industrie ou est portée devant les tribunaux compétents.

VI.2) Traitement des plaintes

Toute plainte concernant des produits fait l'objet d'un examen par le LNE afin de confirmer si la plainte concerne effectivement des produits certifiés. L'entité formulant une plainte doit étayer celle-ci en fournissant des preuves factuelles.

A réception de celles-ci, le LNE les examine et le cas échéant contacte l'entreprise concernée.

L'Entreprise concernée doit alors informer le LNE des suites apportées et tenir à disposition du LNE, les enregistrements relatifs à la plainte ainsi qu'aux actions entreprises pour la résoudre. La vérification de la mise en place des actions annoncées peut faire l'objet d'examens supplémentaires à la charge de l'Entreprise.

Dans le cadre du suivi de l'Entreprise, le LNE examine les enregistrements relatifs aux plaintes et réclamations et vérifie que les corrections et actions correctives appropriées ont été entreprises.

Chapitre VII : Annexes

VII.1) Lexique

Archivage	La fonctionnalité d'archivage, à destination des utilisateurs, a pour objet d'exporter, en garantissant la date de création de l'archive, les données d'encaissement figées dans un format ouvert afin de se prémunir d'une perte des données suites à un problème matériel, une faille de sécurité, un changement de système d'encaissement. Elle ne doit pas être confondue avec seulement une solution de sauvegarde à long terme des données. Il s'agit d'un moyen pour l'assujetti de pouvoir conserver indépendamment du système d'encaissement ses données d'encaissement et pouvoir les communiquer à l'administration fiscale en cas de contrôle.
Archive	Fichier au format ouvert généré par la fonctionnalité d'archivage contenant les données d'encaissement d'une période définie. L'archive ne peut contenir de données d'encaissement sur une période supérieure à un an ou un exercice fiscal.
Authenticité	Caractéristique d'une donnée dont le système est en mesure de vérifier l'identité de l'auteur. Elle peut être assurée grâce aux mécanismes d'empreinte à clé ou de signature.
Chainage	Algorithme consistant à faire dépendre la preuve d'intégrité d'une donnée, de la preuve d'intégrité de la donnée précédente, constituant ainsi une preuve de l'intégrité de l'ensemble des données. Ce mécanisme ne garantit pas l'intégrité du dernier élément et ne permet pas de compter le nombre d'éléments (maillons) manquants lorsque la chaîne est rompue. La preuve d'intégrité peut également être une preuve d'authenticité afin de garantir en plus l'authenticité de la chaîne.
Chiffrage	Évaluation financière, ou action d'écrire ou transcrire en chiffres. À ne pas confondre avec chiffrement.
Chiffrement	Mécanisme cryptographique permettant de garantir la confidentialité de données, en utilisant un chiffre (dans le sens de code secret). Le chiffrement des données n'est pas requis par ce référentiel. À ne pas confondre avec chiffrage.
Clés privées et publiques	Une signature numérique est générée à partir d'une clé privée, qui est un secret cryptographique, et d'un document à signer. La vérification d'une signature est effectuée à partir du document originel et de la clé publique associée au signataire. Connaître une clé publique ne permet pas de retrouver la clé privée correspondante.
Clôture	Fonctionnalité, manuelle ou automatique, offerte par le système d'encaissement qui pour objet de clôturer une période journalière, mensuelle ou annuelle, c'est-à-dire rendre impossible l'enregistrement de nouvelles transactions, de modifier ou d'annuler une transaction sur une période clôturée.
Confidentialité	Caractéristique d'une information ou d'un système visant à s'assurer que leur accès n'est strictement possible qu'aux personnes autorisées. La confidentialité n'est pas requise dans le cadre du référentiel. Elle peut être assurée grâce au chiffrement.

Cryptage	Insérer ou masquer un sens caché dans un texte ou propos, volontairement ou non. Exemple : « décrypter un discours politique ». Pour l'anglicisme, voir chiffrement.
Donnée d'encaissement	Les données d'encaissement correspondent à toutes les données définies à l'exigence n°3, les données d'encaissement correctives définies dans l'exigence n°4, les données du mode école-test définies dans l'exigence n°5 ainsi que les données cumulatives et récapitulatives définies dans l'exigence n°7 ainsi que les données de traçabilité des impressions et réimpressions de justificatifs définies dans l'exigence n°9
Donnée élémentaire	Donnée qui n'est pas obtenue par calcul à partir d'autres données. Toute donnée élémentaire qui concoure à la constitution d'une écriture comptable, à la justification d'un événement ou d'une situation transcrite dans les livres, registres, documents, pièces et déclarations est visée par le droit de contrôle de l'administration fiscale.
Editeur	Personne qui détient le code source du système d'encaissement et qui a la maîtrise de la modification des paramètres impactant les conditions de sécurisation, conservation et archivage des données d'encaissement de celui-ci.
Empreinte / hash / condensat	Résultat d'une fonction qui associe à une donnée de taille arbitraire une donnée de taille fixe. Lorsque l'empreinte est de qualité cryptographique, il n'est pas faisable de calculer l'inverse de cette fonction.
Empreinte à clé	Empreinte cryptographique réalisée en combinant les données sources à un secret d'authentification. Cela permet d'assurer que seul le détenteur du secret peut générer et vérifier une empreinte. Une empreinte à clé permet de garantir l'intégrité d'un document et d'en assurer l'authenticité, sans pouvoir distinguer les identités des détenteurs du secret.
Fonctionnalité de caisse	Fonctionnalité qui consiste à mémoriser et à enregistrer extra-comptablement des paiements reçus en contrepartie d'une vente (de produits ou de services). Si le paiement déclenche concomitamment, automatiquement, obligatoirement, instantanément et sans intervention humaine la passation d'une écriture comptable la fonctionnalité n'est pas considéré comme une fonctionnalité de caisse mais comme une fonctionnalité d'écriture comptable.
Horodatage	Valeur de temps unique croissante monotone indiquant la date et l'heure à laquelle un événement s'est produit. Ces données sont présentées dans un format cohérent, facilitant la comparaison de deux enregistrements différents et le traçage dans le temps.
Imputabilité	Possibilité d'attribuer la responsabilité d'un fait à une personne.
Inaltérabilité	Caractéristique d'un système dont rien ne peut changer les données enregistrées sans traçabilité (i.e. sans que le système ne le détecte). Une altération des données constitue une atteinte à leur intégrité et à leur authenticité.
Intégrité	Caractéristique de données n'ayant subi aucune modification ou destruction, volontaire ou accidentelle.
Journalisation	Enregistrement séquentiel d'événements affectant un processus particulier. C'est un moyen d'assurer la traçabilité des événements.
Justificatif / pièce justificative	Document regroupant des données permettant de justifier le détail de la commande, des ventes, des achats et du mode de paiement d'un produit ou d'une prestation.

Logiciel libre	Logiciel dont les utilisateurs ont un libre usage, une libre étude, une libre modification et une libre distribution. Ces libertés permettent aux utilisateurs d'adapter le logiciel à leurs besoins spécifiques. [Source : BOI-TVA-DECLA-30-10-30]
Mandataire	Personne morale ou physique implantée dans l'Espace Economique Européen (E.E.E) qui a une fonction de représentation du titulaire hors E.E.E et dispose d'un mandat écrit de celui-ci lui signifiant qu'il peut agir en son nom dans le processus de certification suivant les dispositions des présentes règles. Le mandataire peut également être distributeur ou importateur des produits certifiés, ses différentes fonctions sont alors clairement identifiées.
Mode/environnement école/test	Mode ou environnement optionnel d'un système d'encaissement permettant de générer ou de simuler des données afin d'enregistrer des transactions fictives à des fins de tests ou de formation.
Périmètre fiscal	Ensemble exhaustif du code source, des librairies, pilotes et modules impactant les fonctionnalités et exigences énoncées dans le présent référentiel.
Preuve d'authenticité	Donnée qui permet de prouver l'authenticité d'un document. Voir empreinte à clé, signature.
Preuve d'intégrité	Donnée qui permet de prouver l'intégrité d'un document. Voir empreinte, signature.
Purge	Suppression irréversible des données enregistrées sur un système.
Redondance	Méthode consistant à dupliquer tout ou partie de données pour pouvoir les restaurer à leur état d'origine en cas d'altération. Elle peut assurer la disponibilité de l'information qui est la capacité d'un système à rester fonctionnel ou à garder les données accessibles dans le temps.
Secret cryptographique	Un secret cryptographique est une donnée confidentielle utilisée pour chiffrer ou authentifier un document. La confidentialité de ce secret permet de garantir les propriétés (confidentialité ou authenticité) du mécanisme qui l'emploie. Pour être qualifié de cryptographiquement sûr, ce secret doit être généré aléatoirement, ne pas être utilisé pour différents usages, et avoir une taille définie par le mécanisme qui l'emploie.
Signature	Une signature numérique est un mécanisme qui permet de garantir l'intégrité d'un document et d'en assurer l'authenticité. À la différence d'une empreinte à clé, le vérifieur n'a pas besoin de connaître un secret pour vérifier l'authenticité et il ne peut pas usurper l'identité du signataire.
Système d'encaissement	Un système d'encaissement est un système informatique doté d'une fonctionnalité de caisse.

Titulaire	Personne morale qui assure la maîtrise et/ou la responsabilité du respect de l'ensemble des exigences définies dans les présentes règles de certification. Ces exigences couvrent au moins les étapes suivantes : conception, fabrication, assemblage, contrôle qualité, marquage, conditionnement ainsi que la mise sur le marché et précisent les points critiques des différentes étapes. Certaines de ces activités peuvent être réalisées sur le site du titulaire ou sur un autre site par le titulaire lui-même ou par une autre structure avec laquelle il y a une délégation de responsabilités. Cela inclut par exemple des filiales ou des sous-traitants. Quel que soit le site ou le niveau d'externalisation, il importe que le titulaire soit en mesure de présenter l'intégralité des preuves de conformité au référentiel. Le paragraphe 310 du BOI-TVA-DECLA-30-10-30-20160803 indique que le titulaire est l'éditeur du système de caisse. Lorsque le titulaire n'est pas établi dans la communauté européenne, il doit obligatoirement désigner un mandataire.
Total cumulatif / cumul de période	Cumul du chiffre d'affaire décompté depuis l'ouverture de la période concernée. Il s'agit d'un compteur initialisé à 0 à l'ouverture de la période (ou clôture de la période précédente) et dont la valeur est stockée au moment de la fin de la période.
Total perpétuel / cumul perpétuel	Cumul du chiffre d'affaire décompté depuis l'initialisation du système d'encaissement. Il s'agit d'un compteur ne se remettant jamais à, qui n'est pas directement lié à une période mais dont la valeur est enregistrée à un instant t : au moment de chaque clôture (journalière, mensuelle ou annuelle).
TPV	Terminal Point de Vente identifié par un numéro unique (n° de terminal, de caisse, de balance etc.). Un terminal assure l'enregistrement des données d'encaissement localement, temporairement (en attendant le transfert des données vers un système centralisateur) ou dans le respect avec l'exigence n° 16 concernant la conservation des données pendant la durée de 6 ans à partir de la date de la dernière transaction enregistrée sur l'exercice fiscal courant.
Traçabilité	Aptitude à retrouver l'historique, la mise en œuvre ou l'emplacement de ce qui est examiné. Elle est liée à la journalisation et à l'imputabilité.
X	Terme provenant des anciennes caisses enregistreuses actionnées par clé. Lecture simple du chiffre d'affaires de la journée, pouvant être réalisé à tout moment et sans impact sur les données de transactions enregistrées.
Z	Terme provenant des anciennes caisses enregistreuses actionnées par clé. Clôture de caisse de la journée : plus aucune modification des données de transactions enregistrées depuis le dernier Z n'est possible, seuls sont conservés les soldes de caisse (par exemple les espèces encore présentes dans le tiroir-caisse).

VII.2) Tableau de correspondance exigences V1.2 / V1.4

& BOI 04-07-2018	N° cond v1.2	N° exig v1.4
1	/	I.1)
10	/	/
20	/	/
25	/	I.1)
30	/	I.2)
35	/	I.2)
40	/	/
LPF	1	1-2
340	2	20-21
55	/	/
60	3	19
100	8	
70	~~4~~	/
50	5	3
75		
130		
80	6	8
90	7	4
130		
~~110~~	~~9~~	/
120	10	8
130	11	
140	12	
/	/	9
150	13	5
~~160~~	~~14~~	6
170	15	
	16	7
180	17	13
	18	
155		
~~190~~		
~~200~~	19	
210	20	18
	21	
220	22	10-11
	23	10-12
	24	12
	25	17-13
230	26	10
170-240	27	14
250	28	13
250	29	12
260	30	14